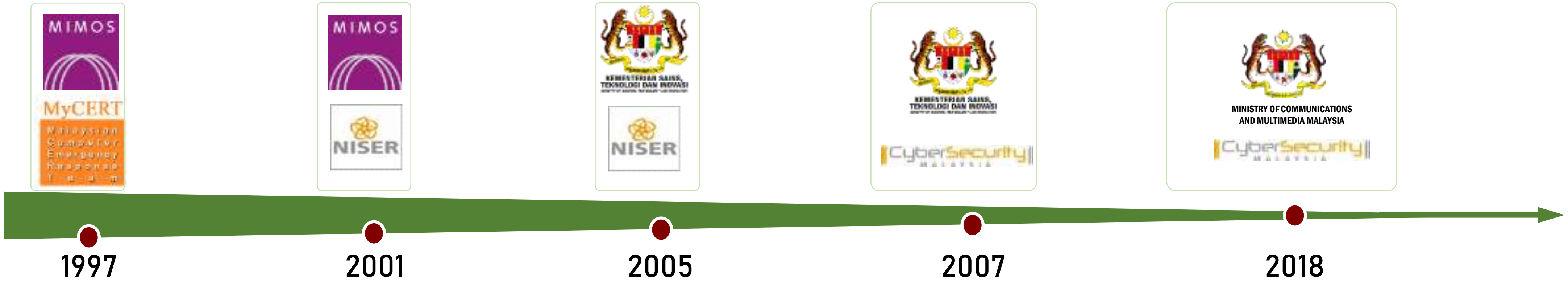
NATIONAL KEY INFORMATION INFRASTRUCTURE EMERGENCY RESPONSE MODEL

DR. ZAHRI YUNOS Chief Operating Officer, CyberSecurity Malaysia

2018 ISC 互联网安全大会 中国 · 北京
Internet Security Conference 2018 Beijing · China
（原 “中国互联网安全大会”）

About CyberSecurity Malaysia

- A technical cyber security agency under the Ministry of Communications and Multimedia Malaysia
- Started operation as the Malaysia Computer Emergency Response Team (MyCERT) in year 1997 and later “rebranded” as CYBERSECURITY MALAYSIA in 2007


MIMOS
MyCERT
Malaysian Computer Emergency Response Team
MIMOS
NISER
KEMENTERIAN SAINS, TEKNOLOGI DAN INOVASI
NISER
KEMENTERIAN SAINS, TEKNOLOGI DAN INOVASI
CyberSecurity MALAYSIA
MINISTRY OF COMMUNICATIONS AND MULTIMEDIA MALAYSIA
CyberSecurity MALAYSIA

1997

2001

2005

2007

2018

NISER was officially registered as CyberSecurity Malaysia (CSM) and put under the purview of MOSTI

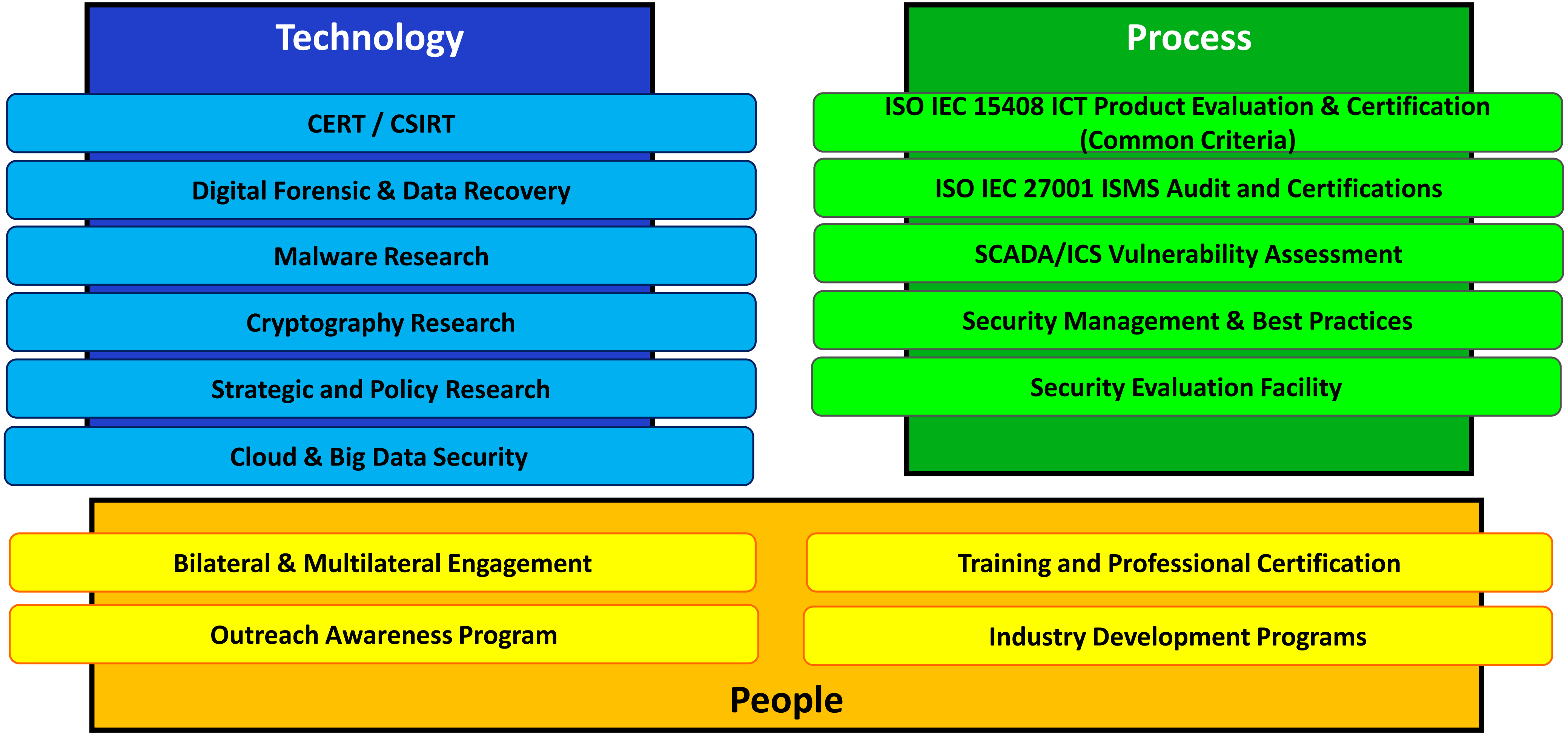
20 Aug 2007

CSM was launched by The Prime Minister of Malaysia

Aug 2018

CSM is put under the purview of Ministry of Communications and Multimedia Malaysia

CyberSecurity Malaysia Strategic Programs



Technology

- CERT / CSIRT
- Digital Forensic & Data Recovery
- Malware Research
- Cryptography Research
- Strategic and Policy Research
- Cloud & Big Data Security

Process

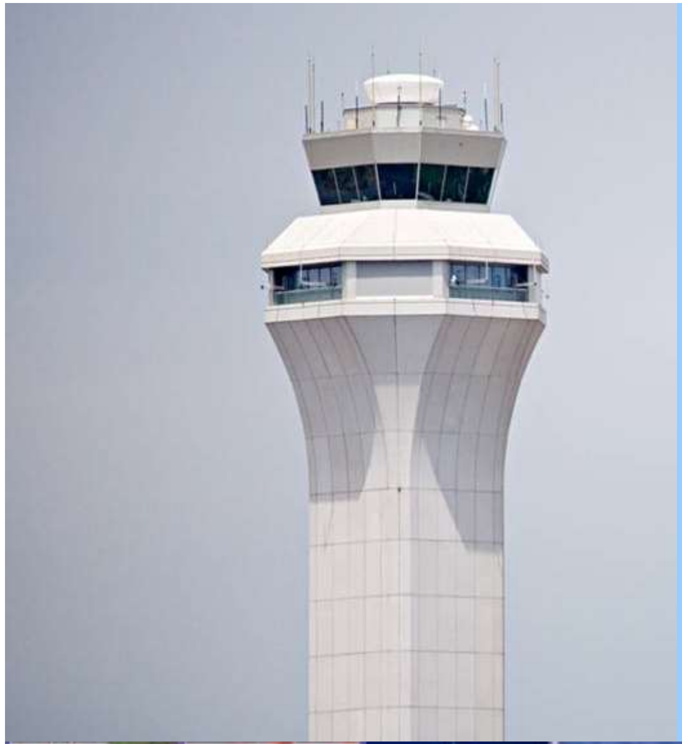
- ISO IEC 15408 ICT Product Evaluation & Certification (Common Criteria)
- ISO IEC 27001 ISMS Audit and Certifications
- SCADA/ICS Vulnerability Assessment
- Security Management & Best Practices
- Security Evaluation Facility

People

- Bilateral & Multilateral Engagement
- Training and Professional Certification
- Outreach Awareness Program
- Industry Development Programs

Legend : 🟦 Technology 🟩 Process 🟨 People

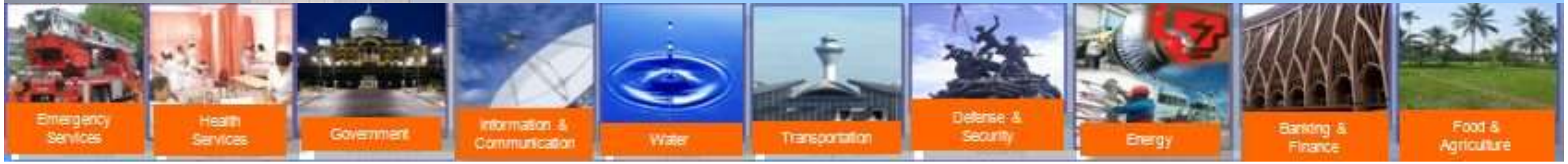
Protection Of Critical National Information Infrastructure (CNII) - Key To Malaysia's E-Sovereignty



CNII:

Assets, systems and functions that are vital to the nation that their incapacity or destruction would have a devastating impact on:

- **National Defence and Security**
- **National Economic Strength**
- **National Image**
- **Government Capabilities to Function**
- **Public Health and Safety**



CNII in Malaysia

VISION

‘Malaysia's Critical National Information Infrastructure shall be secure, resilient and self-reliant. Infused with a culture of security, it will promote stability, social well being and wealth creation’

DEFENCE & SECURITY

TRANSPORTATION

BANKING & FINANCE

HEALTH SERVICES

EMERGENCY SERVICES

CRITICAL NATIONAL INFORMATION INFRASTRUCTURE

Assets (real & virtual), systems and functions that are vital to the nation that their incapacity or destruction would have a devastating impact on

•National defense & security
•National economic strength
•National image
•Government capability to function
•Public health & safety

ENERGY

INFORMATION & COMMUNICATIONS

GOVERNMENT

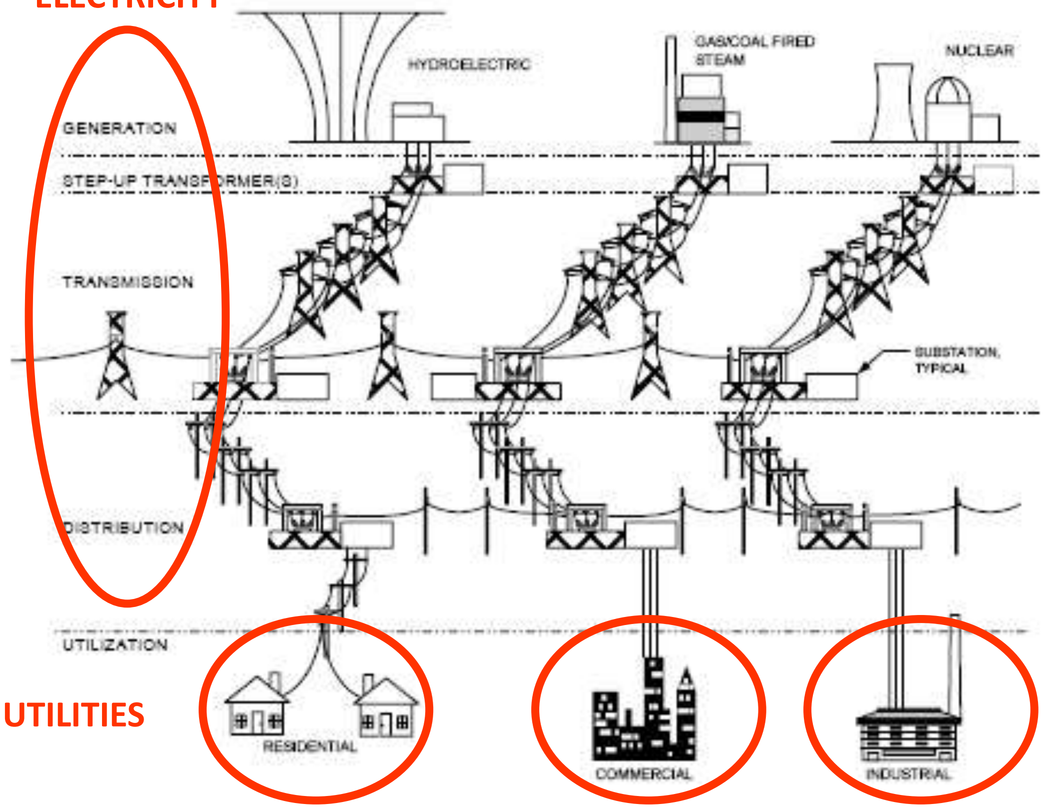
FOOD & AGRICULTURE

WATER

Threats to CNII : Interdependency

The high degree of interdependency between critical infrastructure sectors means failures in one sector can propagate into others.

ELECTRICITY

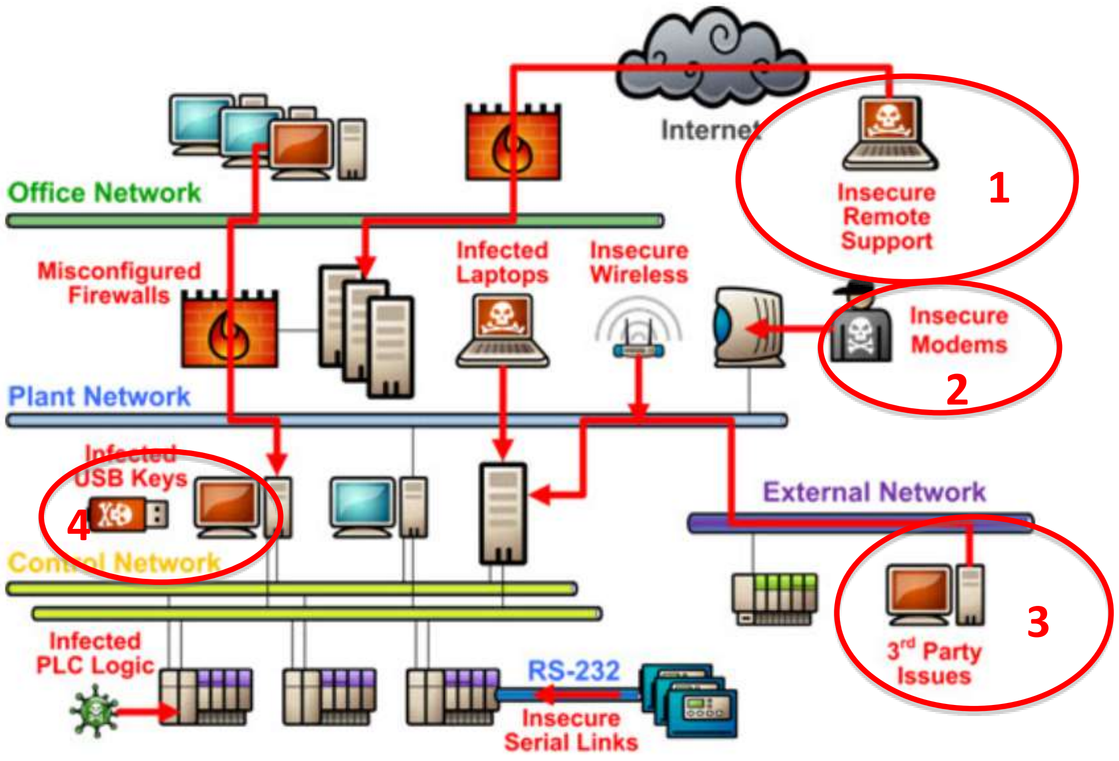


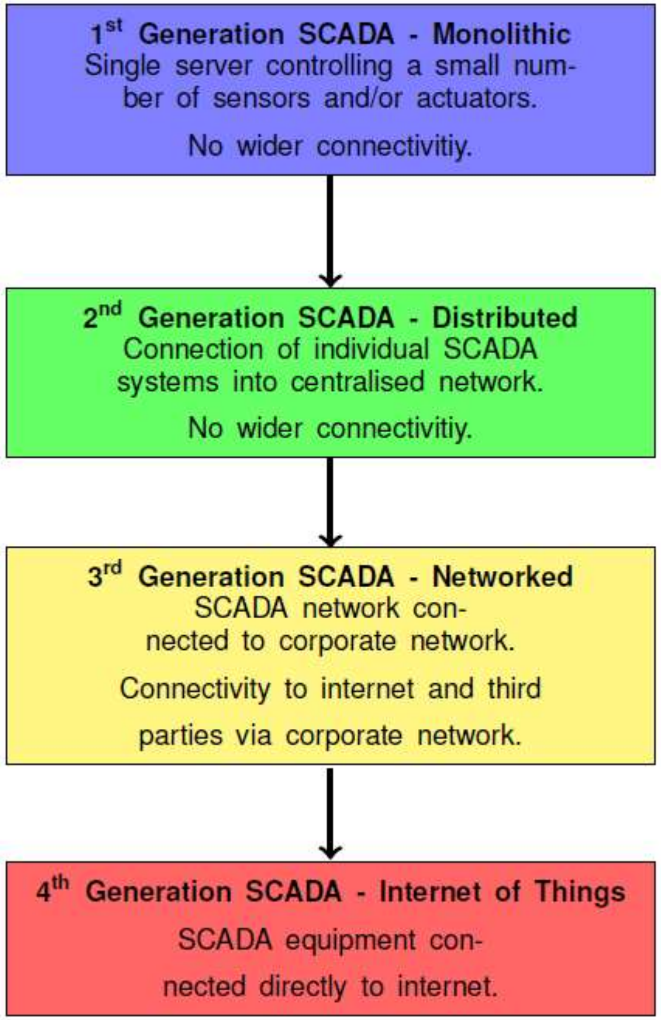
UTILITIES

SECTORS / SERVICES

Threats to CNII : SCADA Systems

SCADA = Supervisory Control & Data Acquisition





1st Generation SCADA - Monolithic
Single server controlling a small number of sensors and/or actuators.

No wider connectivitiy.

2nd Generation SCADA - Distributed
Connection of individual SCADA systems into centralised network.

No wider connectivitiy.

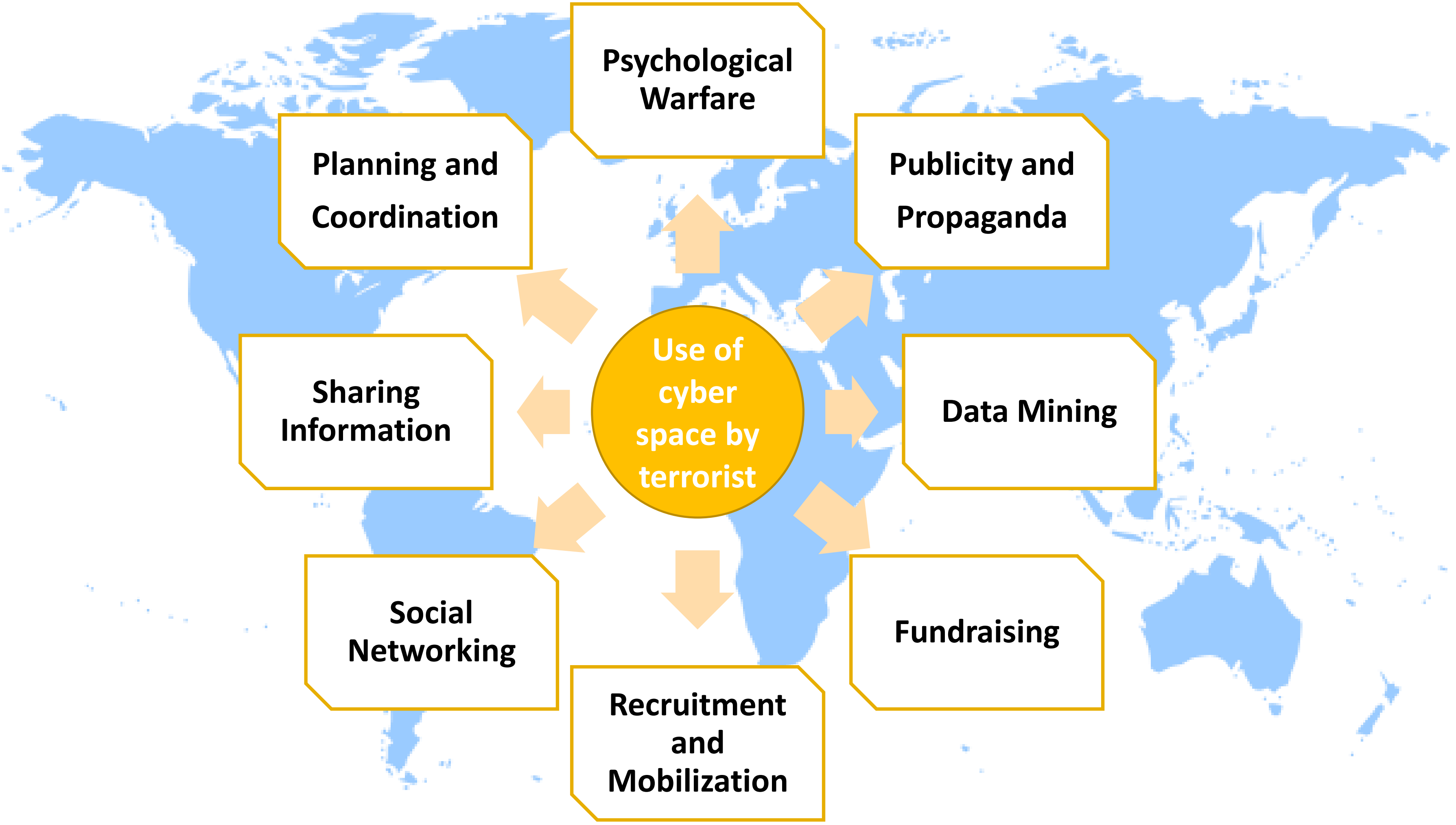
3rd Generation SCADA - Networked
SCADA network connected to corporate network.

Connectivity to internet and third parties via corporate network.

4th Generation SCADA - Internet of Things
SCADA equipment connected directly to internet.

Reference: Using ANSI/ISA-99 Standards to Improve Control System Security by Tofino Security

Threats to CNII : The Use of ICT and Cyberspace by Terrorist



Use of cyber space by terrorist

Psychological Warfare

Publicity and Propaganda

Data Mining

Fundraising

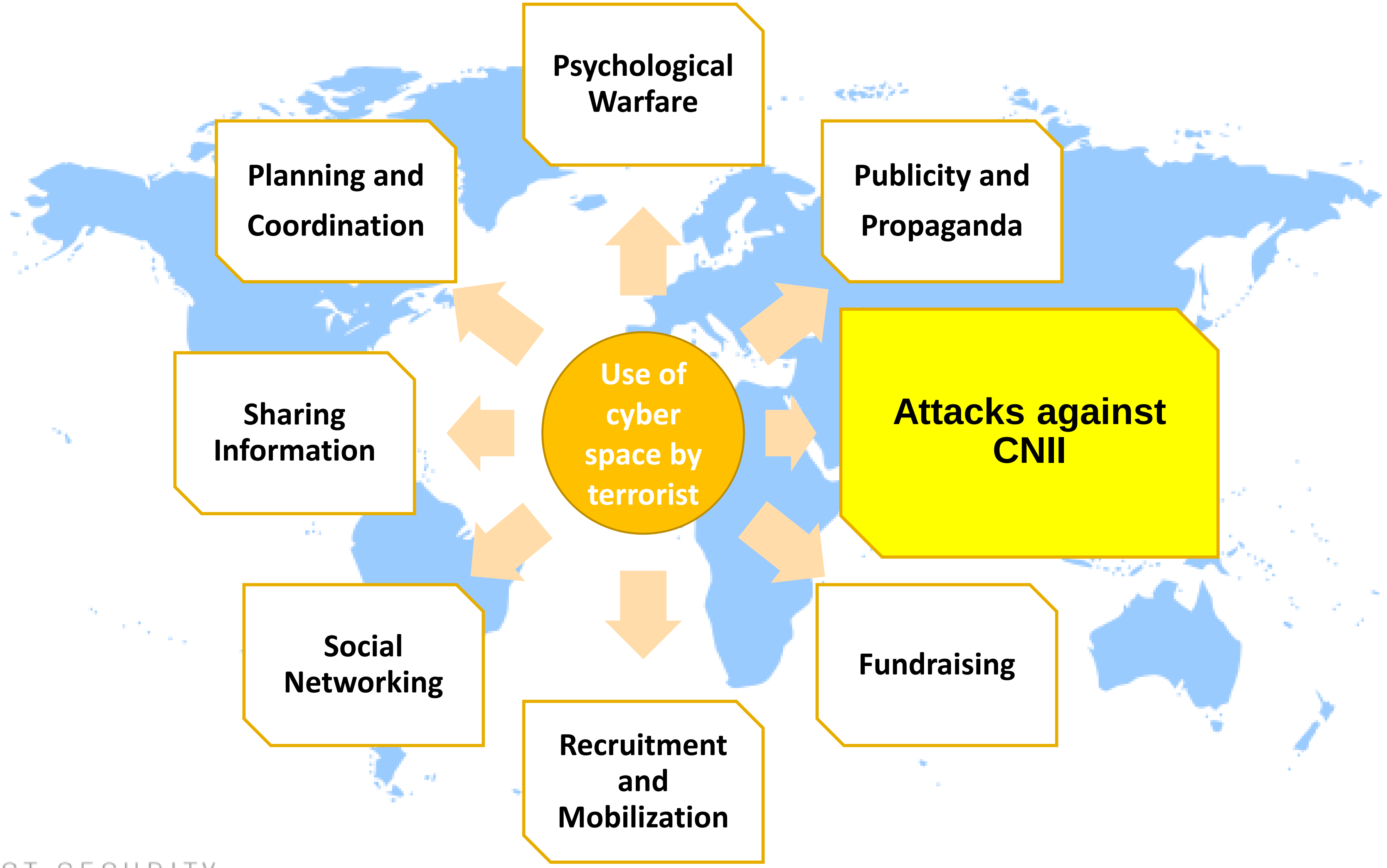
Recruitment and Mobilization

Social Networking

Sharing Information

Planning and Coordination

The perpetrator may utilize the cyberspace for conducting cyber attacks on CNII facilities



Use of cyber space by terrorist

Psychological Warfare

Publicity and Propaganda

Attacks against CNII

Fundraising

Recruitment and Mobilization

Social Networking

Sharing Information

Planning and Coordination

Cyber Threats Come In Various Forms

Technology Related Threats

Hack Threat

Intrusion

Fraud

Spam

Malicious Code

Denial of Service Attack

Stacheldraht DDoS Attack
Internet
Targeted Servers

Cyber Content Related Threats

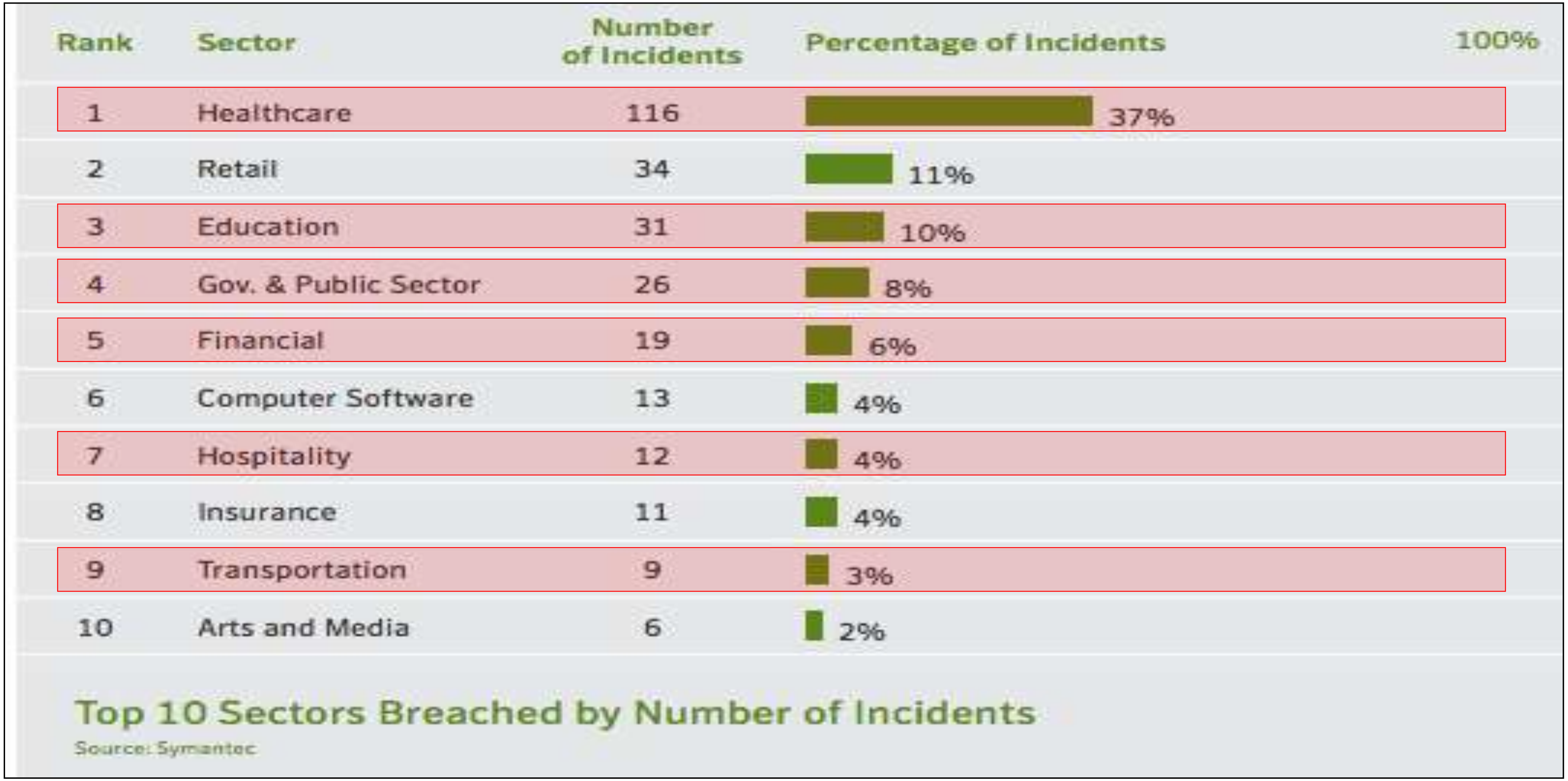
Threats to National Security

Cyber Harassment

Child Porn

Fake News / Defamation

Cyber Incidents By Sectors

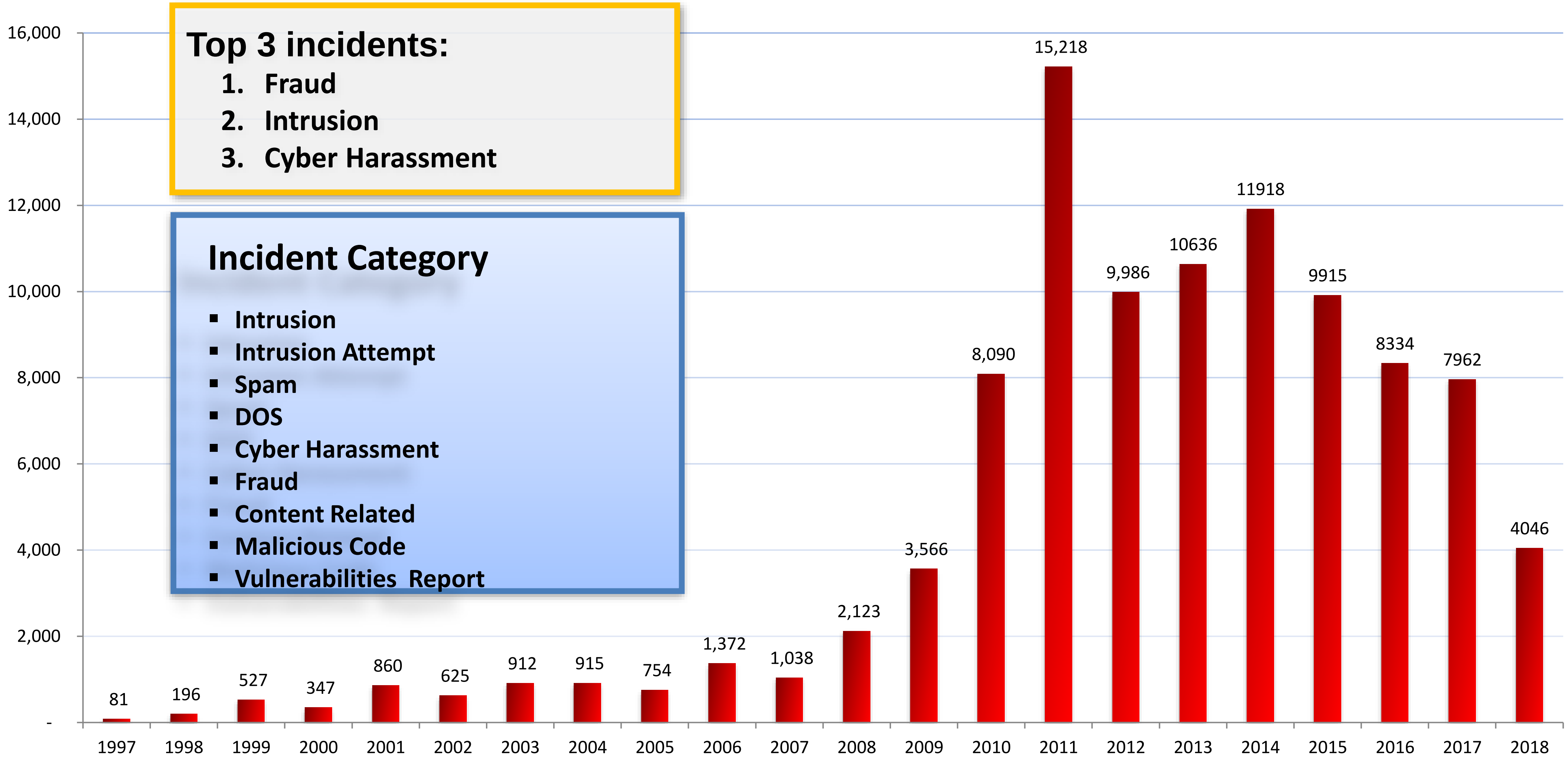


Rank	Sector	Number of Incidents	Percentage of Incidents	100%
1	Healthcare	116	37%	
2	Retail	34	11%	
3	Education	31	10%	
4	Gov. & Public Sector	26	8%	
5	Financial	19	6%	
6	Computer Software	13	4%	
7	Hospitality	12	4%	
8	Insurance	11	4%	
9	Transportation	9	3%	
10	Arts and Media	6	2%	

Top 10 Sectors Breached by Number of Incidents

Source: Symantec

Cyber Security Incidents Reported to CyberSecurity Malaysia



Top 3 incidents:

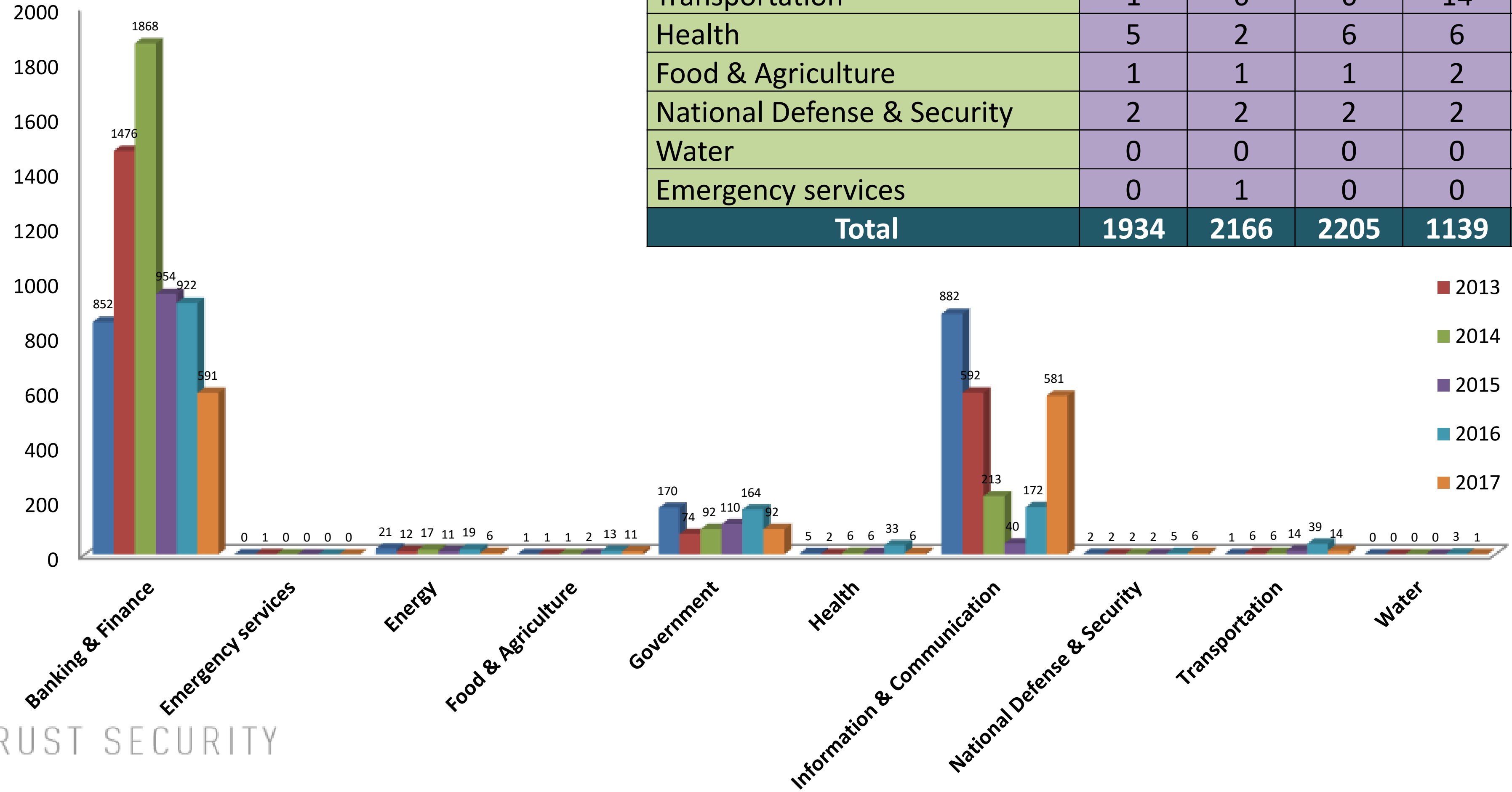
1. **Fraud**
2. **Intrusion**
3. **Cyber Harassment**

Incident Category

- **Intrusion**
- **Intrusion Attempt**
- **Spam**
- **DOS**
- **Cyber Harassment**
- **Fraud**
- **Content Related**
- **Malicious Code**
- **Vulnerabilities Report**

Cyber Incidents by Sector (2012-2017)

	2012	2013	2014	2015	2016	2017	TOTAL
Banking & Finance	852	1476	1868	954	922	591	6663
Information & Communication	882	592	213	40	172	581	2480
Government	170	74	92	110	164	92	702
Energy	21	12	17	11	19	6	86
Transportation	1	6	6	14	39	14	80
Health	5	2	6	6	33	6	58
Food & Agriculture	1	1	1	2	13	11	29
National Defense & Security	2	2	2	2	5	6	19
Water	0	0	0	0	3	1	4
Emergency services	0	1	0	0	0	0	1
Total	1934	2166	2205	1139	1370	1308	10122



Source : www.mycert.org.my

Issues and Challenges

1) Legal challenges

- Not mandatory for reporting cyber incidents
- Cross border jurisdiction
- Identity / ownership

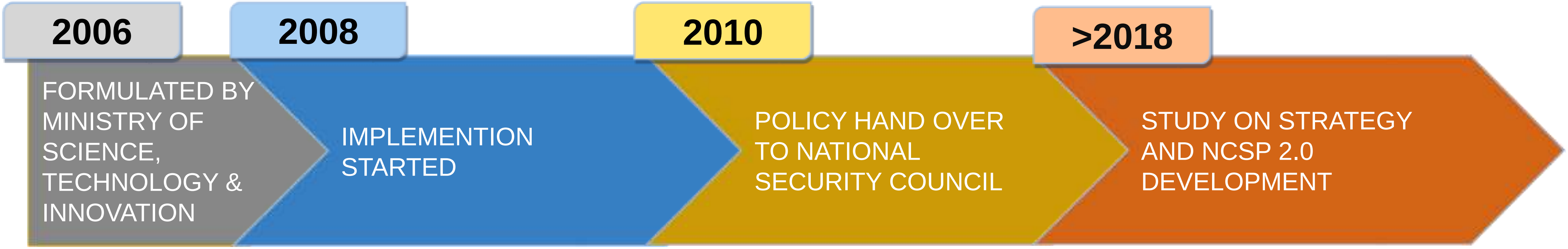
2) Technical challenges

- Anti forensics technology
- Anonymizer technology
- Internet of Things technology

3) Governance challenges

- Inter-working relationship
- Budget and funding
- Syndicate / organized crime network

The National Cyber Security Policy



2006

FORMULATED BY MINISTRY OF SCIENCE, TECHNOLOGY & INNOVATION

2008

IMPLEMENTION STARTED

2010

POLICY HAND OVER TO NATIONAL SECURITY COUNCIL

>2018

STUDY ON STRATEGY AND NCSP 2.0 DEVELOPMENT

Vision

Malaysia's **Critical National Information Infrastructure** shall be secure, resilient and self-reliant. Infused with a culture of security, it will promote stability, social well being and wealth creation

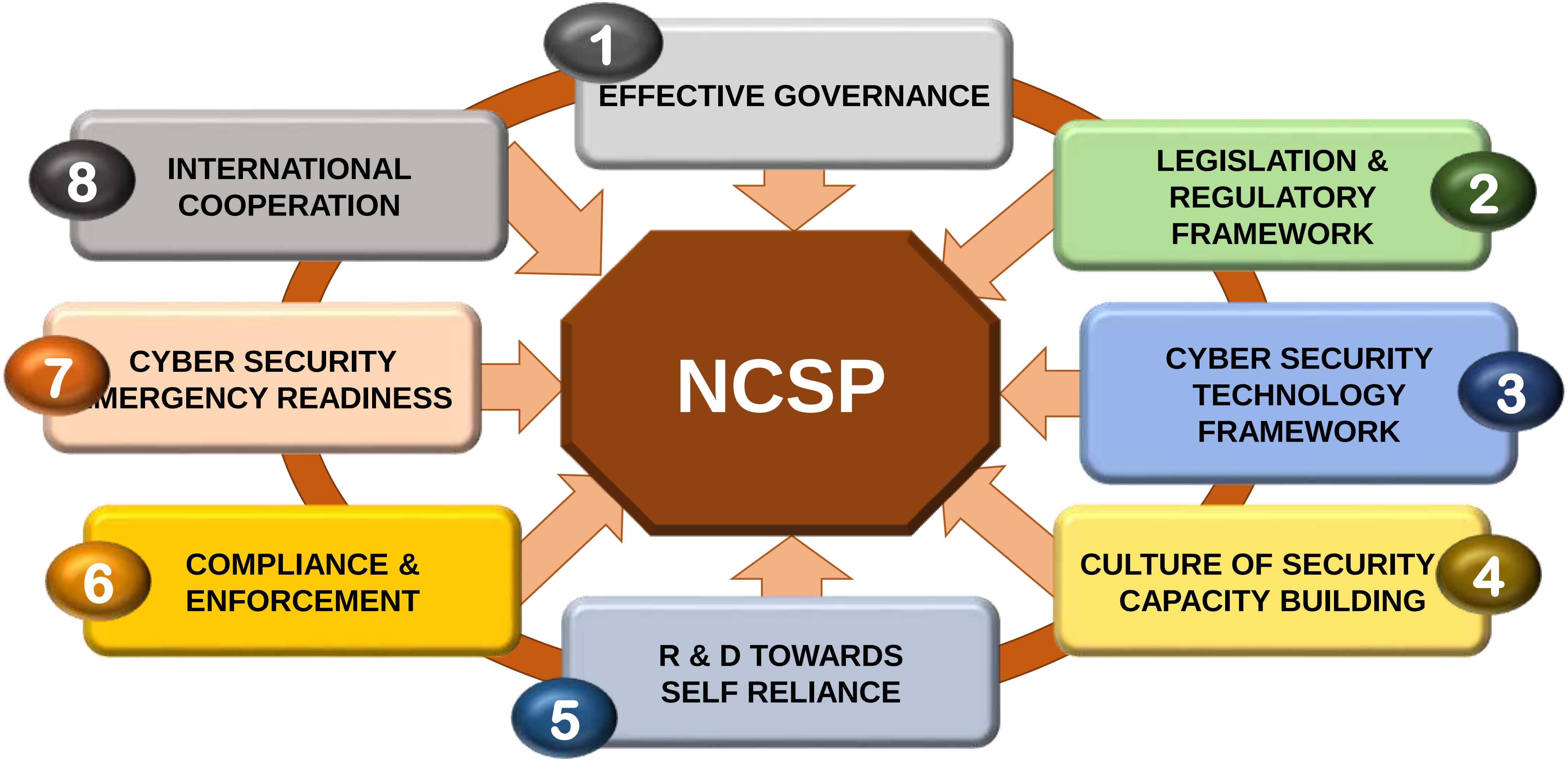
Objective

i. Address the risks to the **Critical National Information Infrastructure (CNII)**

ii. To ensure that critical infrastructure are protected to a level that is commensurate with the risks

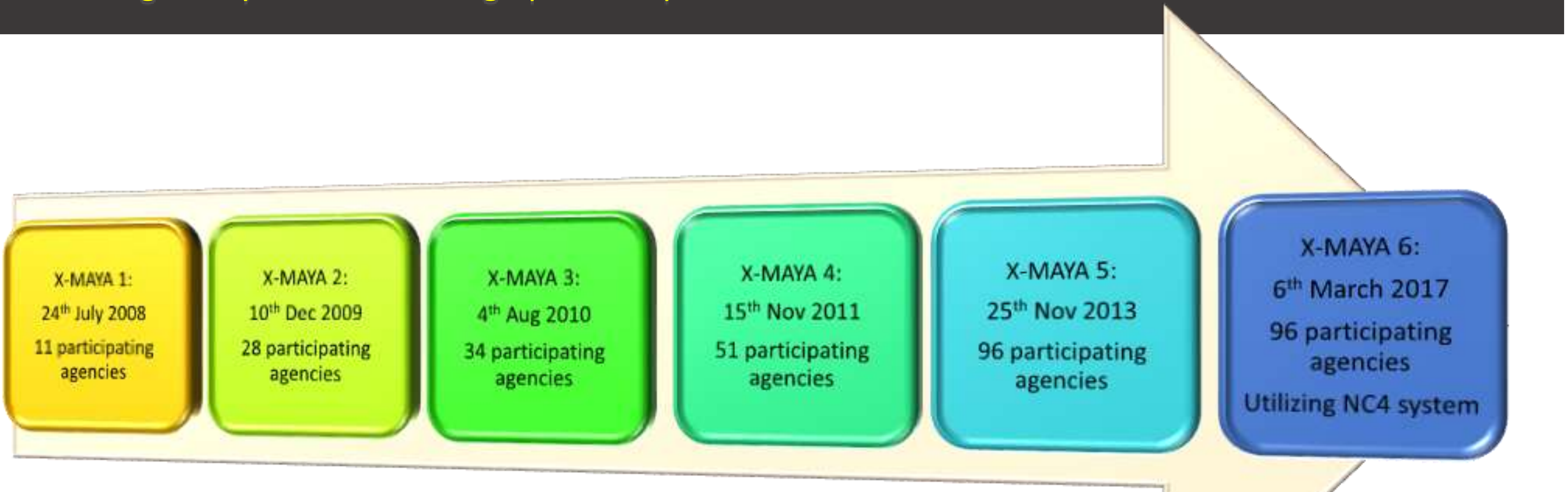
iii. To develop and establish a comprehensive program and a series of frameworks

The National Cyber Security Policy
- Policy Thrust


1
EFFECTIVE GOVERNANCE
2
LEGISLATION & REGULATORY FRAMEWORK
3
CYBER SECURITY TECHNOLOGY FRAMEWORK
4
CULTURE OF SECURITY CAPACITY BUILDING
5
R & D TOWARDS SELF RELIANCE
6
COMPLIANCE & ENFORCEMENT
7
CYBER SECURITY MERGENCY READINESS
8
INTERNATIONAL COOPERATION
NCSP

Policy Thrust 7: National Cyber Crisis Management Plan

Framework that outline the strategy for cyber attacks mitigation & response among malaysia’s CNII through public & private collaboration and coordination



X-MAYA 1: 24th July 2008 11 participating agencies

X-MAYA 2: 10th Dec 2009 28 participating agencies

X-MAYA 3: 4th Aug 2010 34 participating agencies

X-MAYA 4: 15th Nov 2011 51 participating agencies

X-MAYA 5: 25th Nov 2013 96 participating agencies

X-MAYA 6: 6th March 2017 96 participating agencies Utilizing NC4 system

Exercise objective:

1.Examine the effectiveness, identifying the gaps and improve Communication Procedures, Responses and Coordination of NCCMP

2.Familiarize CNII agencies on cyber incident handling mechanisms

3.Familiarize communication between CNII agencies during cyber incidents.

Requirements for CSIRT in Organization in Malaysia

In 2013, the National Security Council of Malaysia (NSC) released the guideline *"NSC Directive 24: National Cyber Crisis Management Mechanism."*

This directive specifies the requirement for all government agencies to establish their own CSIRT as one of the initiatives to manage cyber incidents

In 2013, the latest version of the ISMS standard (27001:2013(E)) contains three additional sub clauses under paragraph A16.1, which emphasize on response and assessment of information security incidents:

1. *A 16.1.5 Response to information security incidents*
2. *A 16.1.6 Learning from information security incidents*
3. *A 16.1.7 Collection of evidence*

1. Our Services: CyberDEF

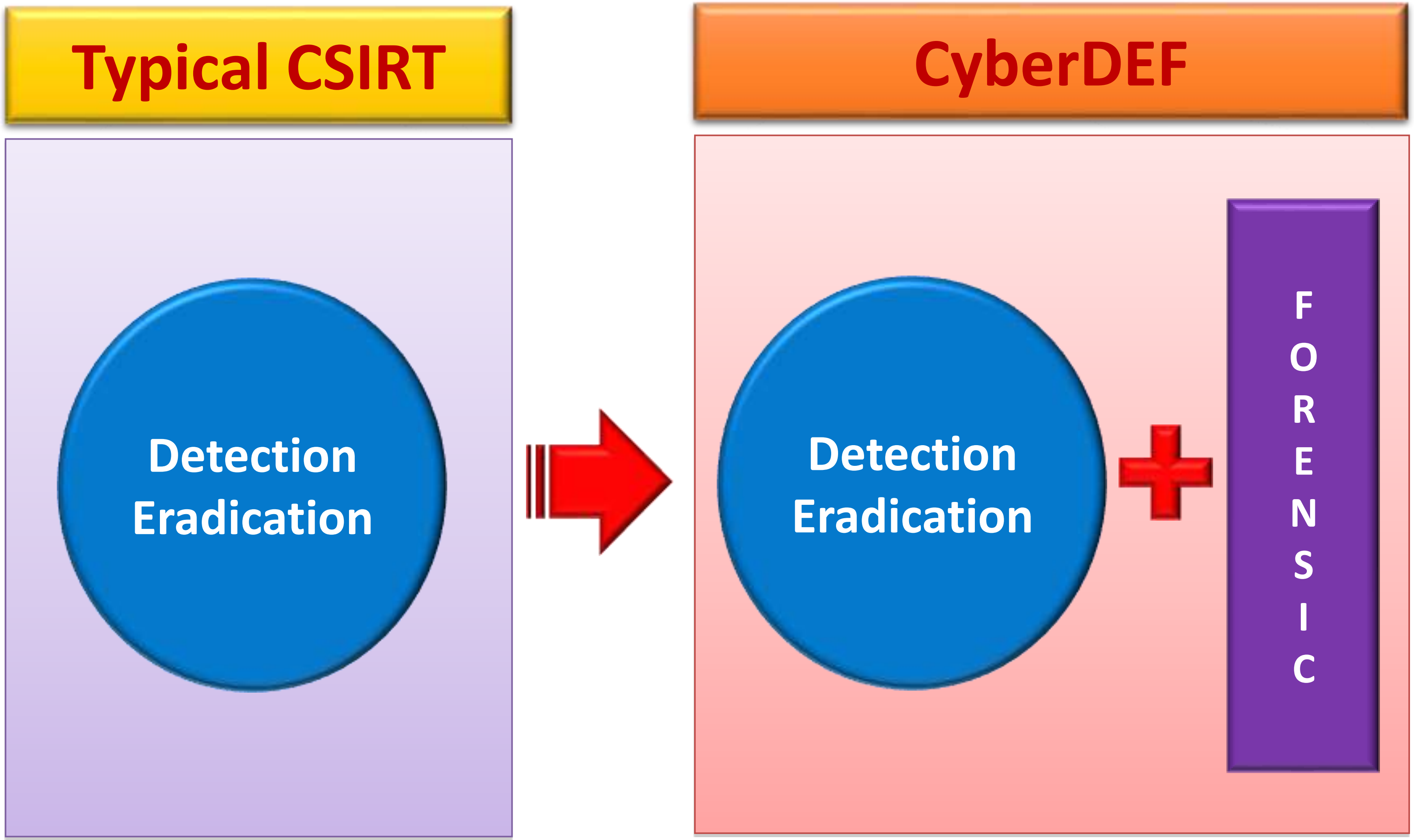
D *“detection of cyber threat”*

E *“eradication of cyber threat”*

This stage is iterative, return to “D” or “E” to improve the technique further

F *“forensic analysis of cyber threat”*

CyberDEF (cont…)



Typical CSIRT

Detection
Eradication

CyberDEF

Detection
Eradication

FORENSIC

CyberDEF (cont…)

Detection

Identify any loopholes, vulnerabilities and existing threats

1. Sensors
2. Sandbox
3. Analytics
4. Visualization

Eradication

Close loopholes, patch vulnerabilities and neutralize existing threats

Perform cyber threats exercise or drill to test the feasibility and resiliency of the new defense / prevention system

Forensics

1. E-Discovery
2. Root cause analysis
3. Investigation
4. Forensics readiness
5. Forensic compliance

CyberDEF (cont…)

Why CyberDEF is unique?

3 Technical Departments

Consists of **3 technical departments** :

1. Secure Technology Services Department (STS)
2. Digital Forensic Department (DF)
3. Malaysia Computer Emergency Response Team (MyCERT)

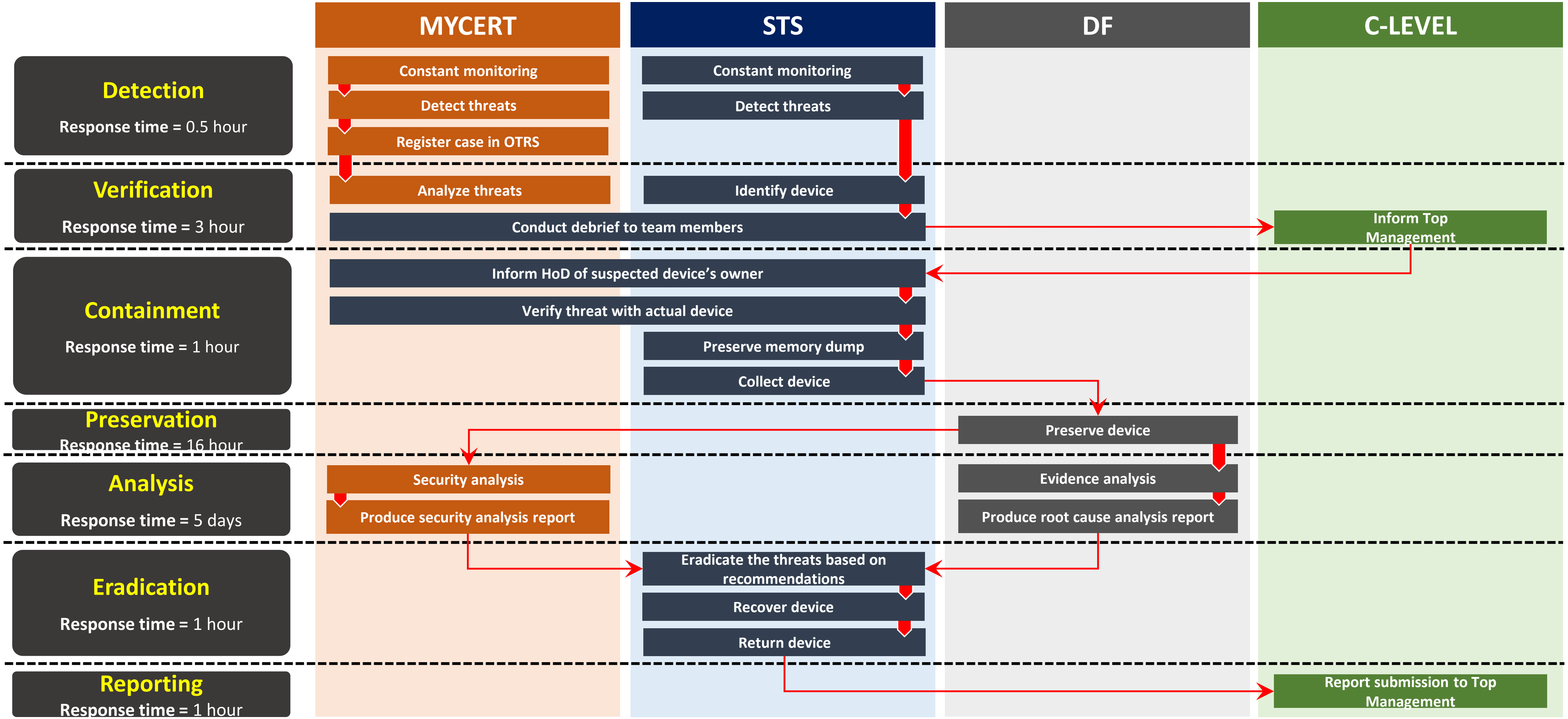
Centralized Governance

Effective **centralized governance** because all of the 3 departments are under the Cyber Security Responsive Services Division

Forensic Element

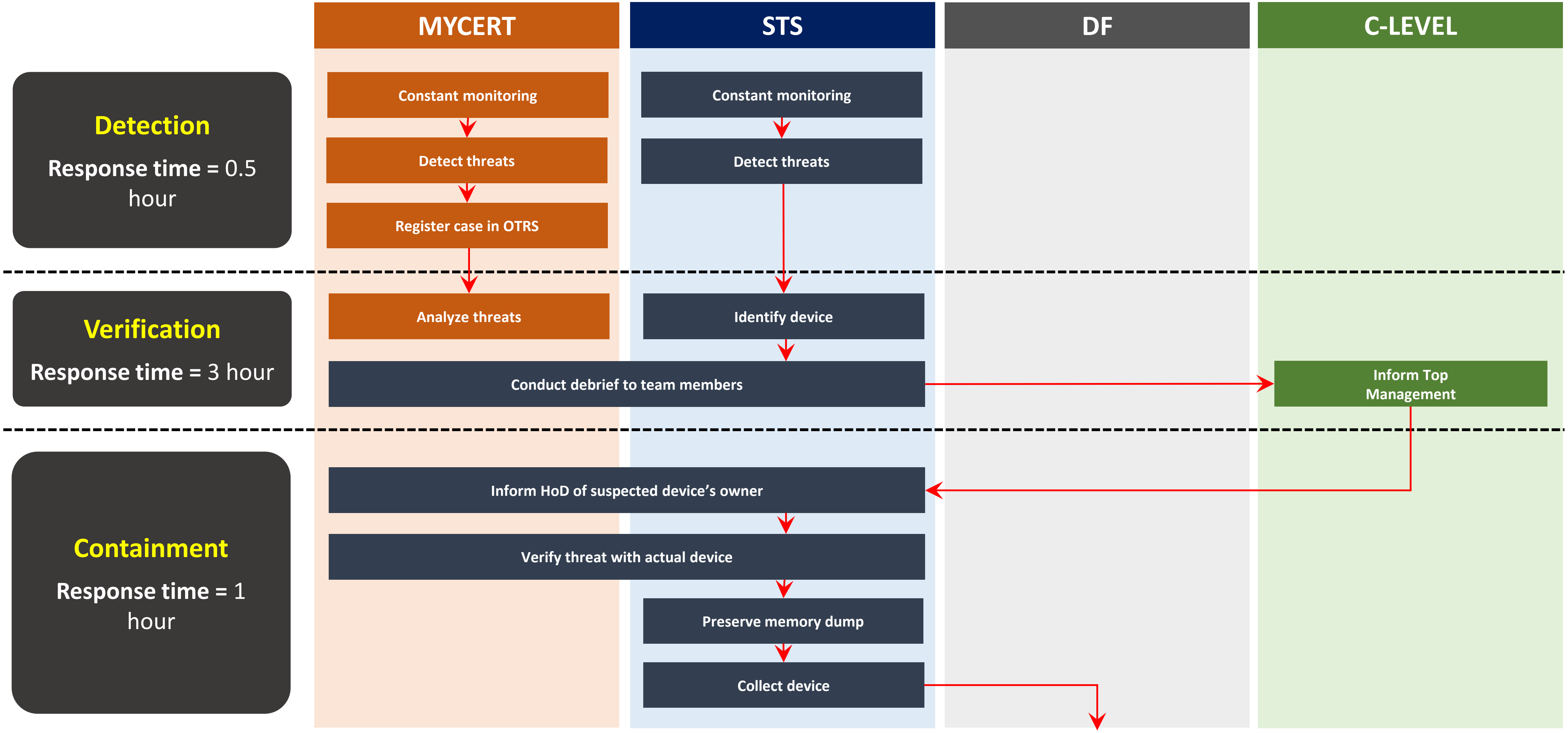
Forensic element **incorporated** in the services offered

CSIRT Management Workflow

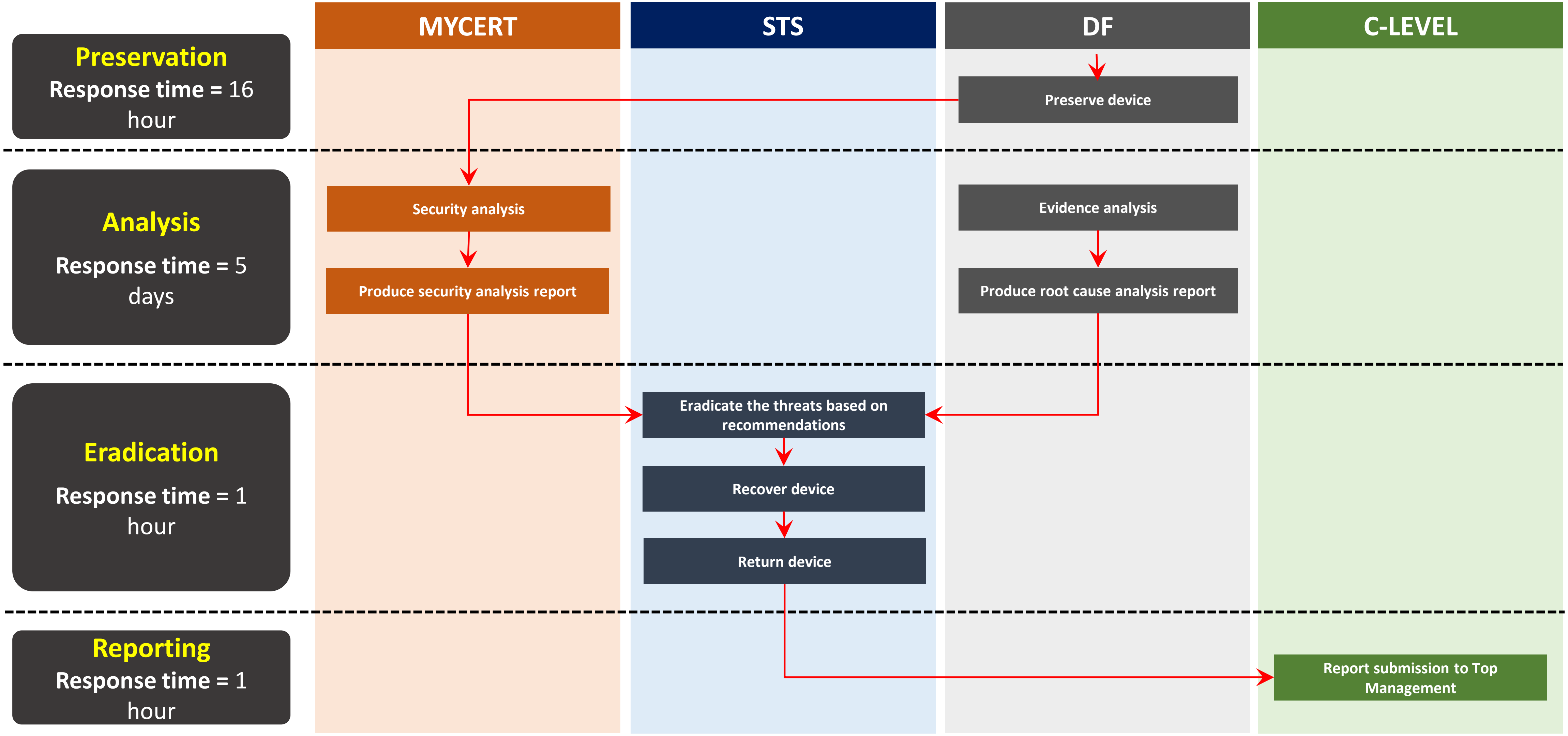


	MYCERT	STS	DF	C-LEVEL
Detection Response time = 0.5 hour	Constant monitoring Detect threats Register case in OTRS	Constant monitoring Detect threats		
Verification Response time = 3 hour	Analyze threats Conduct debrief to team members	Identify device		Inform Top Management
Containment Response time = 1 hour	Inform HoD of suspected device’s owner Verify threat with actual device	Preserve memory dump Collect device		
Preservation Response time = 16 hour			Preserve device	
Analysis Response time = 5 days	Security analysis Produce security analysis report		Evidence analysis Produce root cause analysis report	
Eradication Response time = 1 hour		Eradicate the threats based on recommendations Recover device Return device		
Reporting Response time = 1 hour				Report submission to Top Management

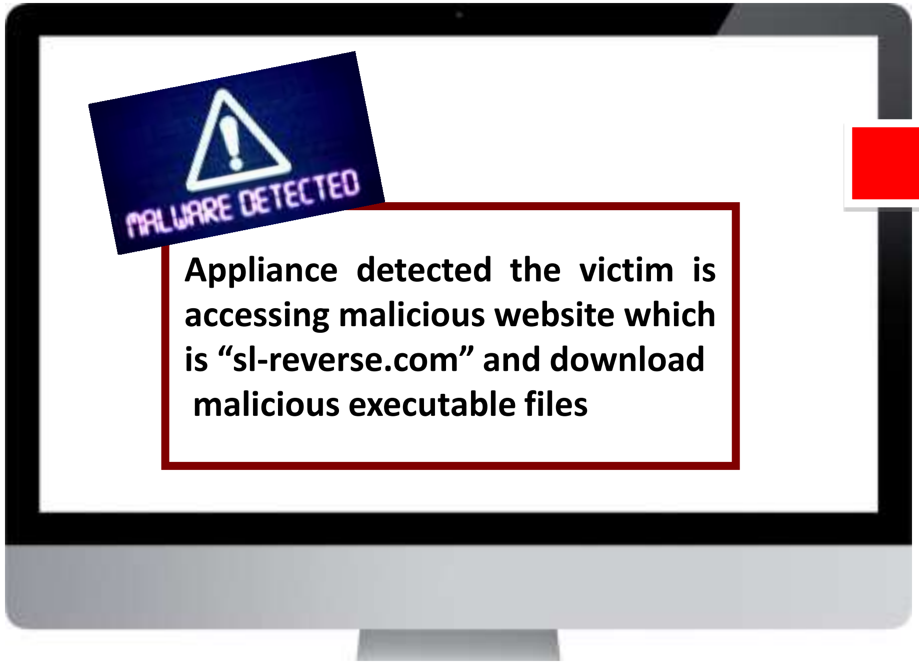
CSIRT Management Workflow



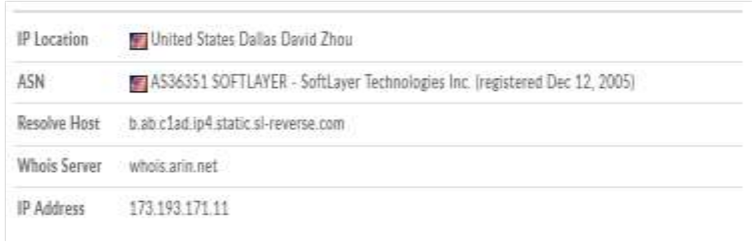
CSIRT Management Workflow



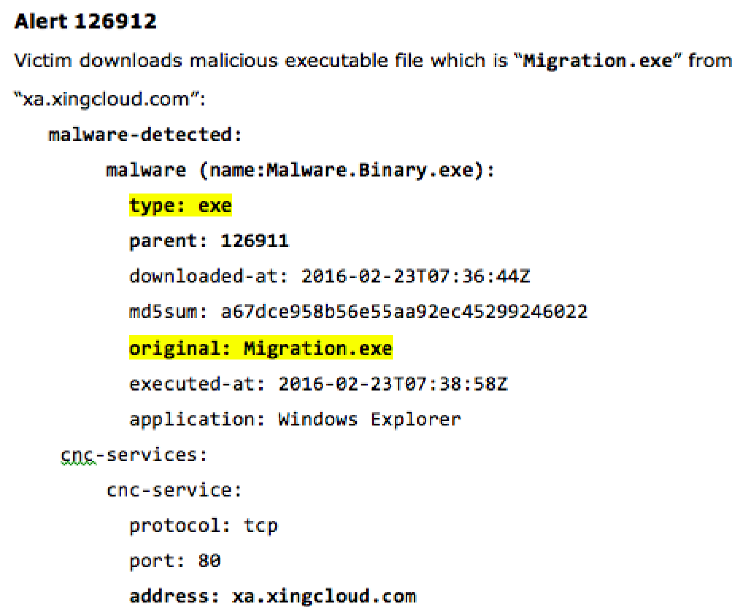
Case Study: Detection



Appliance detected the victim is accessing malicious website which is “sl-reverse.com” and download malicious executable files



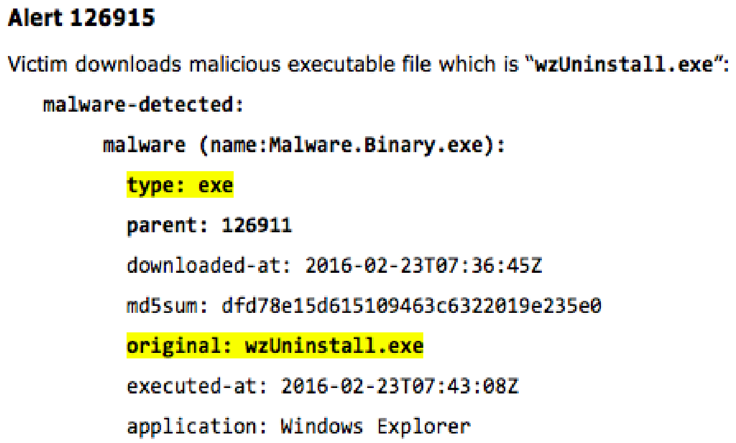
IP Location	United States Dallas David Zhou
ASN	AS36351 SOFTLAYER - SoftLayer Technologies Inc. (registered Dec 12, 2005)
Resolve Host	b.ab.c1ad.ip4.static.sl-reverse.com
Whois Server	whois.arin.net
IP Address	173.193.171.11



Alert 126912

Victim downloads malicious executable file which is “**Migration.exe**” from “xa.xingcloud.com”:

```
malware-detected:
    malware (name:Malware.Binary.exe):
      type: exe
      parent: 126911
      downloaded-at: 2016-02-23T07:36:44Z
      md5sum: a67dce958b56e55aa92ec45299246022
      original: Migration.exe
      executed-at: 2016-02-23T07:38:58Z
      application: Windows Explorer
 cnc-services:
    cnc-service:
      protocol: tcp
      port: 80
      address: xa.xingcloud.com
```



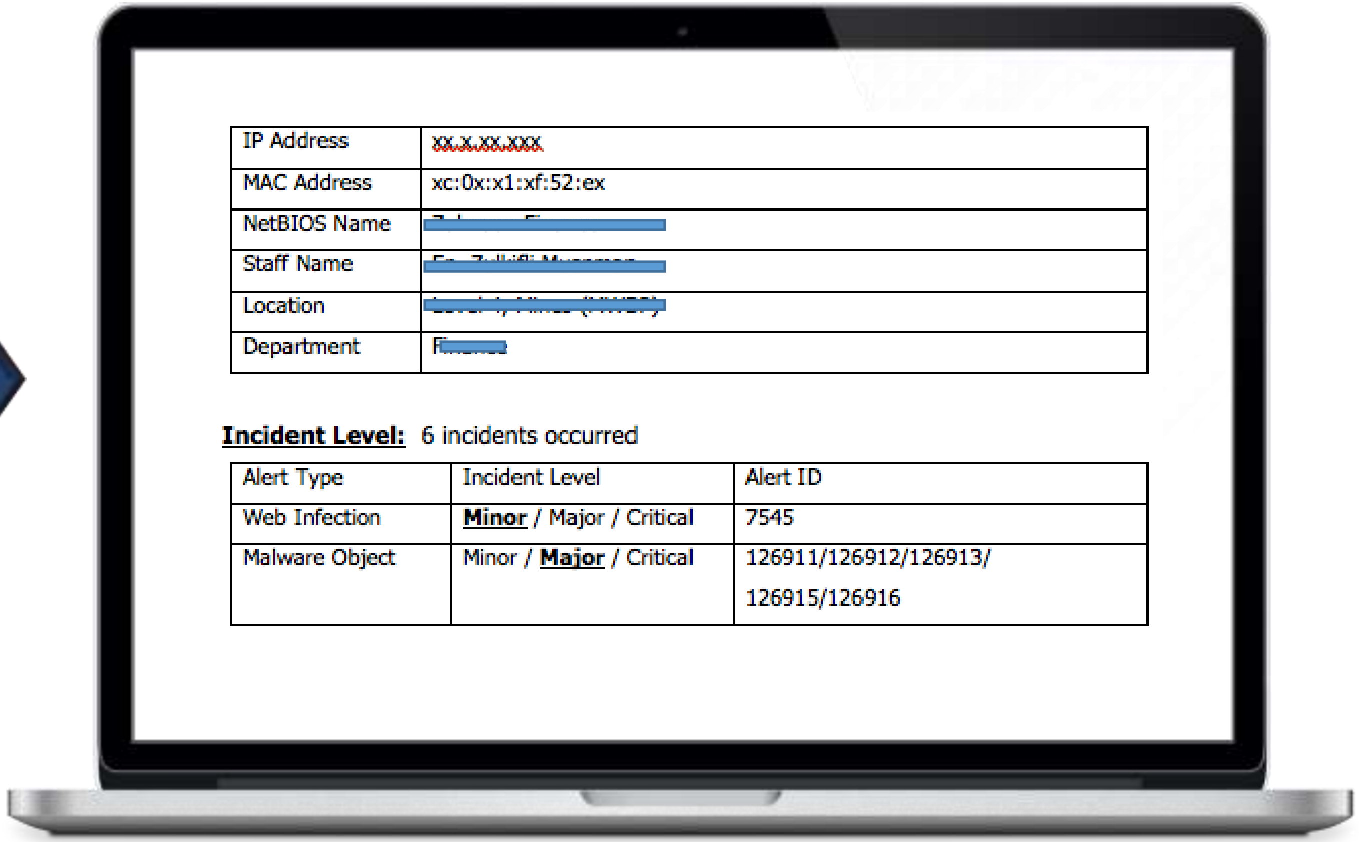
Alert 126915

Victim downloads malicious executable file which is “**wzUninstall.exe**”:

```
malware-detected:
     malware (name:Malware.Binary.exe):
       type: exe
       parent: 126911
       downloaded-at: 2016-02-23T07:36:45Z
       md5sum: dfd78e15d615109463c6322019e235e0
       original: wzUninstall.exe
       executed-at: 2016-02-23T07:43:08Z
       application: Windows Explorer
```

Case Study: Detection (Cont …)

Affected device identified



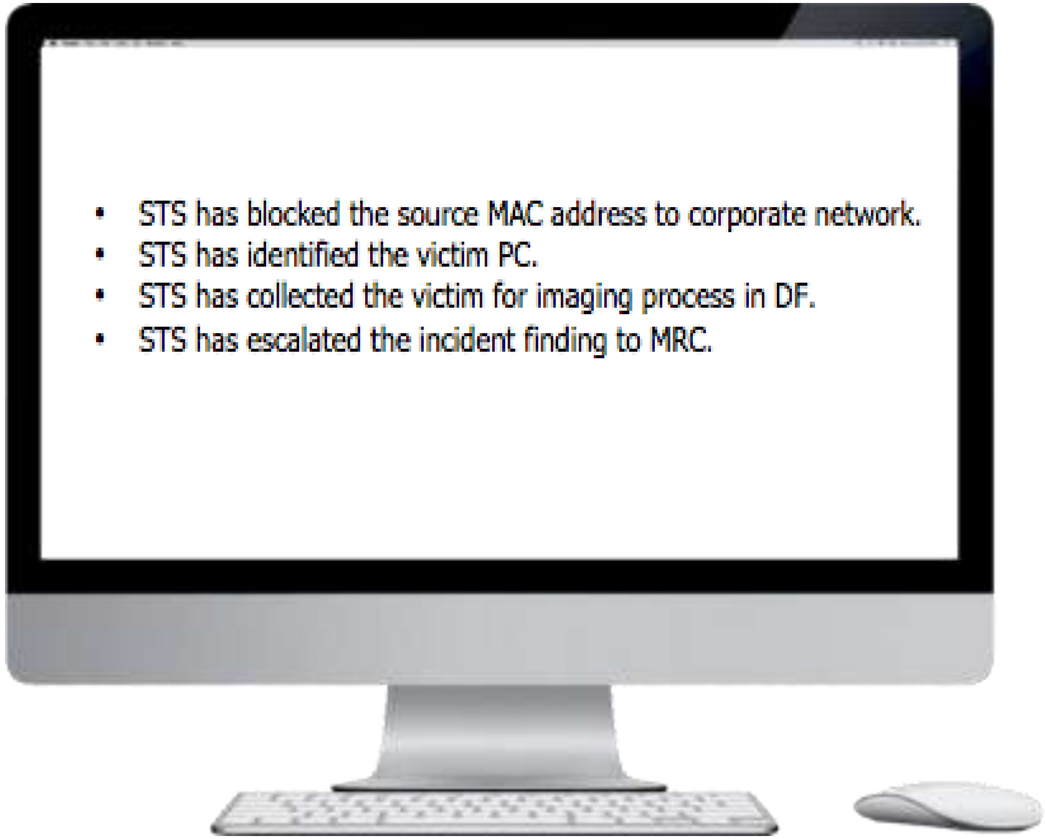
IP Address	xx.x.xx.xxx
MAC Address	xc:0x:x1:xf:52:ex
NetBIOS Name	[redacted]
Staff Name	[redacted]
Location	[redacted]
Department	[redacted]

Incident Level: 6 incidents occurred

Alert Type	Incident Level	Alert ID
Web Infection	**Minor** / Major / Critical	7545
Malware Object	Minor / **Major** / Critical	126911/126912/126913/ 126915/126916

Case Study: Eradication

Eradicate the malware

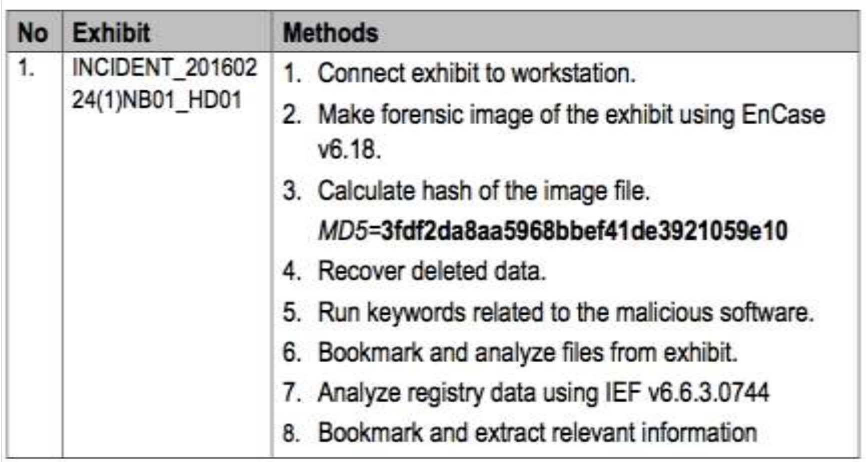


- STS has blocked the source MAC address to corporate network.
- STS has identified the victim PC.
- STS has collected the victim for imaging process in DF.
- STS has escalated the incident finding to MRC.

Case Study: Forensics

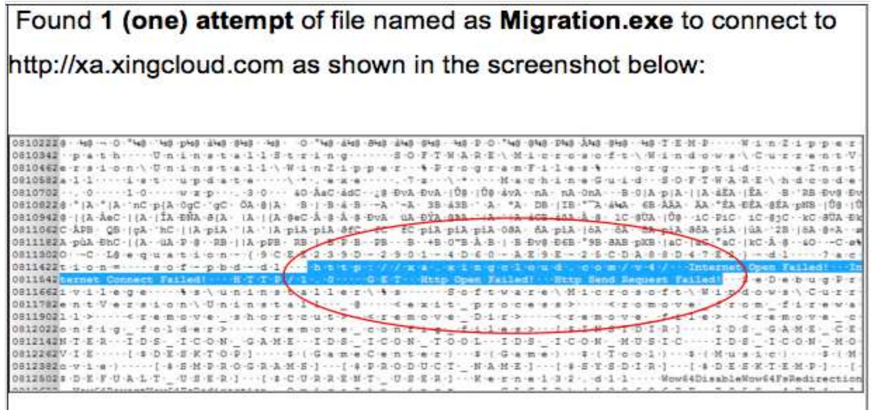
Analysis

Extract metadata & registry info from malicious file and conduct forensics analysis



No	Exhibit	Methods
1.	INCIDENT_20160224(1)NB01_HD01	1. Connect exhibit to workstation. 2. Make forensic image of the exhibit using EnCase v6.18. 3. Calculate hash of the image file. *MD5*=3fdf2da8aa5968bbef41de3921059e10 4. Recover deleted data. 5. Run keywords related to the malicious software. 6. Bookmark and analyze files from exhibit. 7. Analyze registry data using IEF v6.6.3.0744 8. Bookmark and extract relevant information

Findings

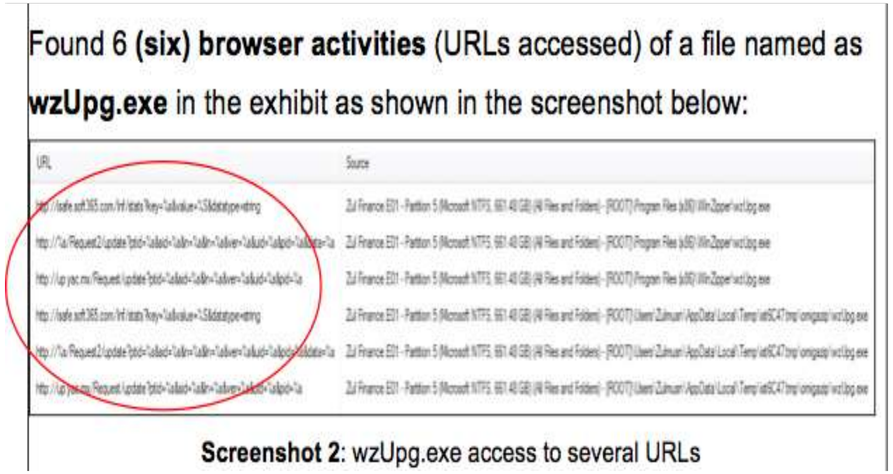


Found **1 (one) attempt** of file named as **Migration.exe** to connect to http://xa.xingcloud.com as shown in the screenshot below:

```
0810222 [illegible] ·T·E·M·P·····W·i·n·Z·i·p·p·e·r
0810342 ··p·a·t·h·····U·n·i·n·s·t·a·l·l·S·t·r·i·n·g·······S·O·F·T·W·A·R·E·\·M·i·c·r·o·s·o·f·t·\·W·i·n·d·o·w·s·\·C·u·r·r·e·n·t·V
0810462 e·r·s·i·o·n·\·U·n·i·n·s·t·a·l·l·\·W·i·n·Z·i·p·p·e·r···%·P·r·o·g·r·a·m·F·i·l·e·s·%·····o·r·g···-·p·t·i·d·:·····e·I·n·s·t
0810582 a·l·l·····i·s·t···u·p·d·a·t·e·····\·*·.·e·x·e·····.·7·z···\·*·····M·a·c·h·i·n·e·G·u·i·d···S·O·F·T·W·A·R·E·\·h·d·c·o·d·e
0810702 ···.·0·····1·0·····w·z·p·····3·0··· [illegible]
0810822 [illegible]
0810942 [illegible]
0811062 [illegible]
0811182 [illegible]
0811302 O···C··L@·e·q·u·a·t·i·o·n···(·9·C·E·1·2·3·9·D·-·2·9·0·1·-·4·D·6·0·-·A·E·9·E·-·2·5·C·D·A·8·8·D·4·7·E·A·)·-·d·l·····?·a·c
0811422 t·i·o·n·=·····s·o·f·-·p·b·d·-·d·l·····h·t·t·p·:·/·/·x·a·.·x·i·n·g·c·l·o·u·d·.·c·o·m·/·v·4·/···Internet Open Failed!···In
0811542 ternet Connect Failed!····H·T·T·P·/·1·.·0·····G·E·T···Http Open Failed!···Http Send Request Failed!·····e·D·e·b·u·g·P·r
0811662 i·v·i·l·e·g·e·····%·s·\·u·n·i·n·s·t·a·l·l·e·r·\·%·s·······S·o·f·t·w·a·r·e·\·M·i·c·r·o·s·o·f·t·\·W·i·n·d·o·w·s·\·C·u·r·r
0811782 e·n·t·V·e·r·s·i·o·n·\·U·n·i·n·s·t·a·l·l···_·@·····<·e·x·i·t·_·p·r·o·c·e·s·s·>·····<·r·e·m·o·v·e·_·f·r·o·m·_·f·i·r·e·w·a
0811902 l·l·>·····<·r·e·m·o·v·e·_·s·h·o·r·t·c·u·t·>···<·r·e·m·o·v·e·_·D·i·r·>·····<·r·e·m·o·v·e·_·f·i·l·e·>···<·r·e·m·o·v·e·_·c
0812022 o·n·f·i·g·_·f·o·l·d·e·r·>·····<·r·e·m·o·v·e·_·c·o·n·f·i·g·_·f·i·l·e·s·>···[·$·I·N·S·T·D·I·R·]·····I·D·S·_·G·A·M·E·_·C·E
0812142 N·T·E·R···I·D·S·_·I·C·O·N·_·G·A·M·E···I·D·S·_·I·C·O·N·_·T·O·O·L···I·D·S·_·I·C·O·N·_·M·U·S·I·C·····I·D·S·_·I·C·O·N·_·M·O
0812262 V·I·E·····[·$·D·E·S·K·T·O·P·]·····$·(·G·a·m·e·C·e·n·t·e·r·)···$·(·G·a·m·e·)···$·(·T·o·o·l·)···$·(·M·u·s·i·c·)·····$·(·M
0812382 o·v·i·e·)·····[·$·S·M·P·R·O·G·R·A·M·S·]···[·$·P·R·O·D·U·C·T·_·N·A·M·E·]···[·$·S·Y·S·D·I·R·]···[·$·D·E·S·K·T·E·M·P·]···[·
0812502 $·D·E·F·U·A·L·T·_·U·S·E·R·]···[·$·C·U·R·R·E·N·T·_·U·S·E·R·]···K·e·r·n·e·l·3·2·.·d·l·l·····Wow64DisableWow64FsRedirection
```

Case Study: Forensics (Cont …)

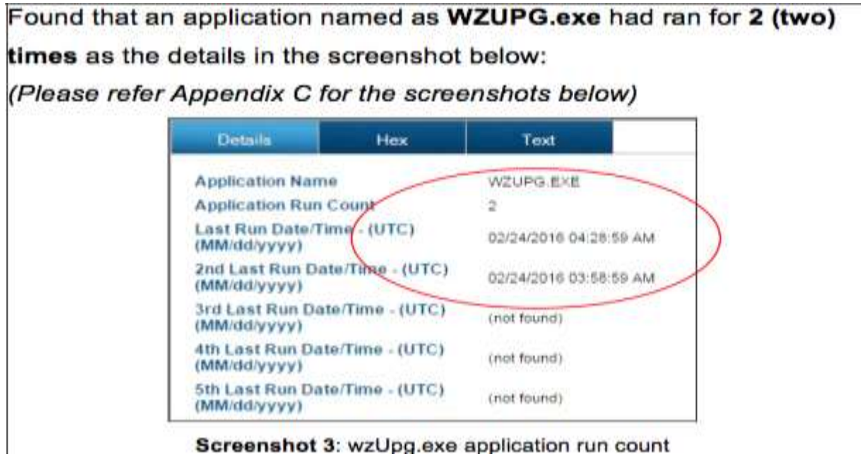
Findings



Found 6 **(six) browser activities** (URLs accessed) of a file named as **wzUpg.exe** in the exhibit as shown in the screenshot below:

URL	Source
http://safe.soft365.com/inf/stats?key=%a&value=%1.5&datatype=string	Zul Finance E01 - Partition 5 (Microsoft NTFS, 661.40 GB) (All Files and Folders) - [ROOT]\Program Files (x86)\WinZipper\wzUpg.exe
http://%a/Request2/update?pbid=%a&aid=%a&n=%a&h=%a&ver=%a&uid=%a&pid=%a&data=%a	Zul Finance E01 - Partition 5 (Microsoft NTFS, 661.40 GB) (All Files and Folders) - [ROOT]\Program Files (x86)\WinZipper\wzUpg.exe
http://up.yac.mx/Request/update?pbid=%a&aid=%a&h=%a&ver=%a&uid=%a&pid=%a	Zul Finance E01 - Partition 5 (Microsoft NTFS, 661.40 GB) (All Files and Folders) - [ROOT]\Program Files (x86)\WinZipper\wzUpg.exe
http://safe.soft365.com/inf/stats?key=%a&value=%1.5&datatype=string	Zul Finance E01 - Partition 5 (Microsoft NTFS, 661.40 GB) (All Files and Folders) - [ROOT]\Users\Zulmuri\AppData\Local\Temp\is6C47.tmp\omigazip\wzUpg.exe
http://%a/Request2/update?pbid=%a&aid=%a&n=%a&h=%a&ver=%a&uid=%a&pid=%a&data=%a	Zul Finance E01 - Partition 5 (Microsoft NTFS, 661.40 GB) (All Files and Folders) - [ROOT]\Users\Zulmuri\AppData\Local\Temp\is6C47.tmp\omigazip\wzUpg.exe
http://up.yac.mx/Request/update?pbid=%a&aid=%a&h=%a&ver=%a&uid=%a&pid=%a	Zul Finance E01 - Partition 5 (Microsoft NTFS, 661.40 GB) (All Files and Folders) - [ROOT]\Users\Zulmuri\AppData\Local\Temp\is6C47.tmp\omigazip\wzUpg.exe

Screenshot 2: wzUpg.exe access to several URLs



Found that an application named as **WZUPG.exe** had ran for **2 (two) times** as the details in the screenshot below:

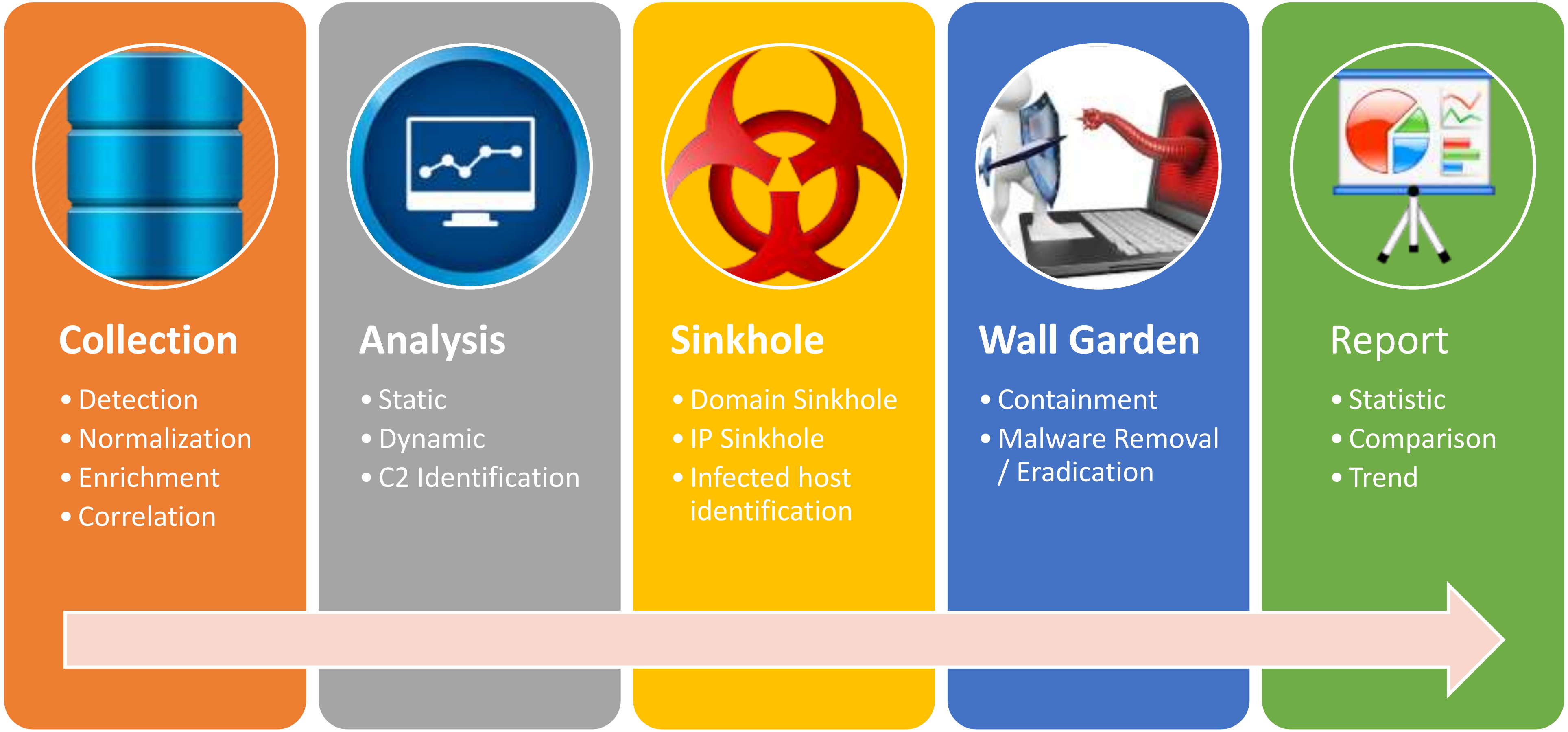
(Please refer Appendix C for the screenshots below)

Application Name	WZUPG.EXE
Application Run Count	2
Last Run Date/Time - (UTC) (MM/dd/yyyy)	02/24/2016 04:28:59 AM
2nd Last Run Date/Time - (UTC) (MM/dd/yyyy)	02/24/2016 03:58:59 AM
3rd Last Run Date/Time - (UTC) (MM/dd/yyyy)	(not found)
4th Last Run Date/Time - (UTC) (MM/dd/yyyy)	(not found)
5th Last Run Date/Time - (UTC) (MM/dd/yyyy)	(not found)

Screenshot 3: wzUpg.exe application run count

2. Our Services: CMERP
Coordinated Malware Eradication & Remediation Project

OBJECTIVE : To **reduce** the number of **Malware infection** in Malaysia



Collection

- Detection
- Normalization
- Enrichment
- Correlation

Analysis

- Static
- Dynamic
- C2 Identification

Sinkhole

- Domain Sinkhole
- IP Sinkhole
- Infected host identification

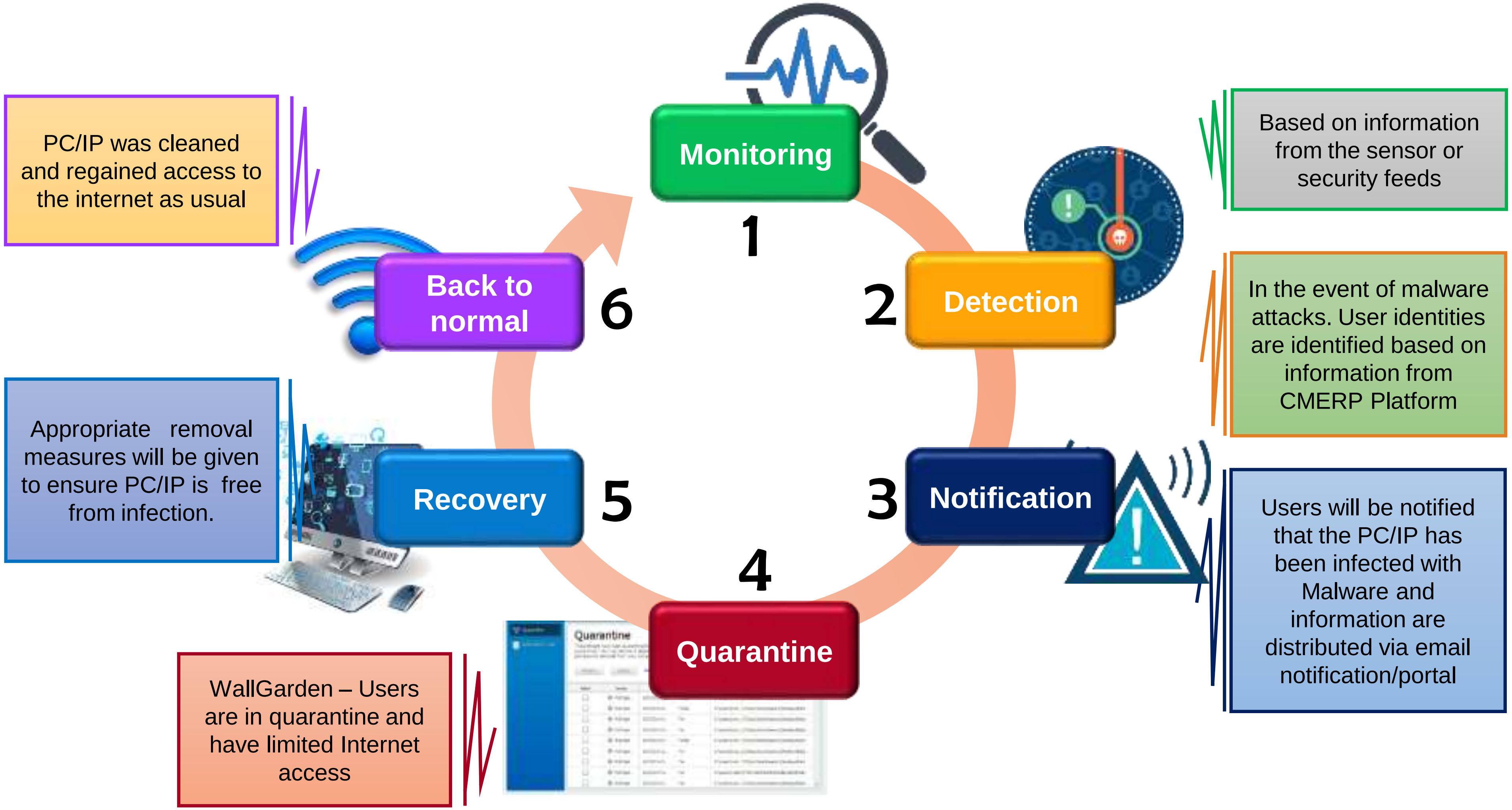
Wall Garden

- Containment
- Malware Removal / Eradication

Report

- Statistic
- Comparison
- Trend

CMERP Ecosystem



Monitoring

1

Based on information from the sensor or security feeds

Detection

2

In the event of malware attacks. User identities are identified based on information from CMERP Platform

Notification

3

Users will be notified that the PC/IP has been infected with Malware and information are distributed via email notification/portal

Quarantine

4

WallGarden – Users are in quarantine and have limited Internet access

Recovery

5

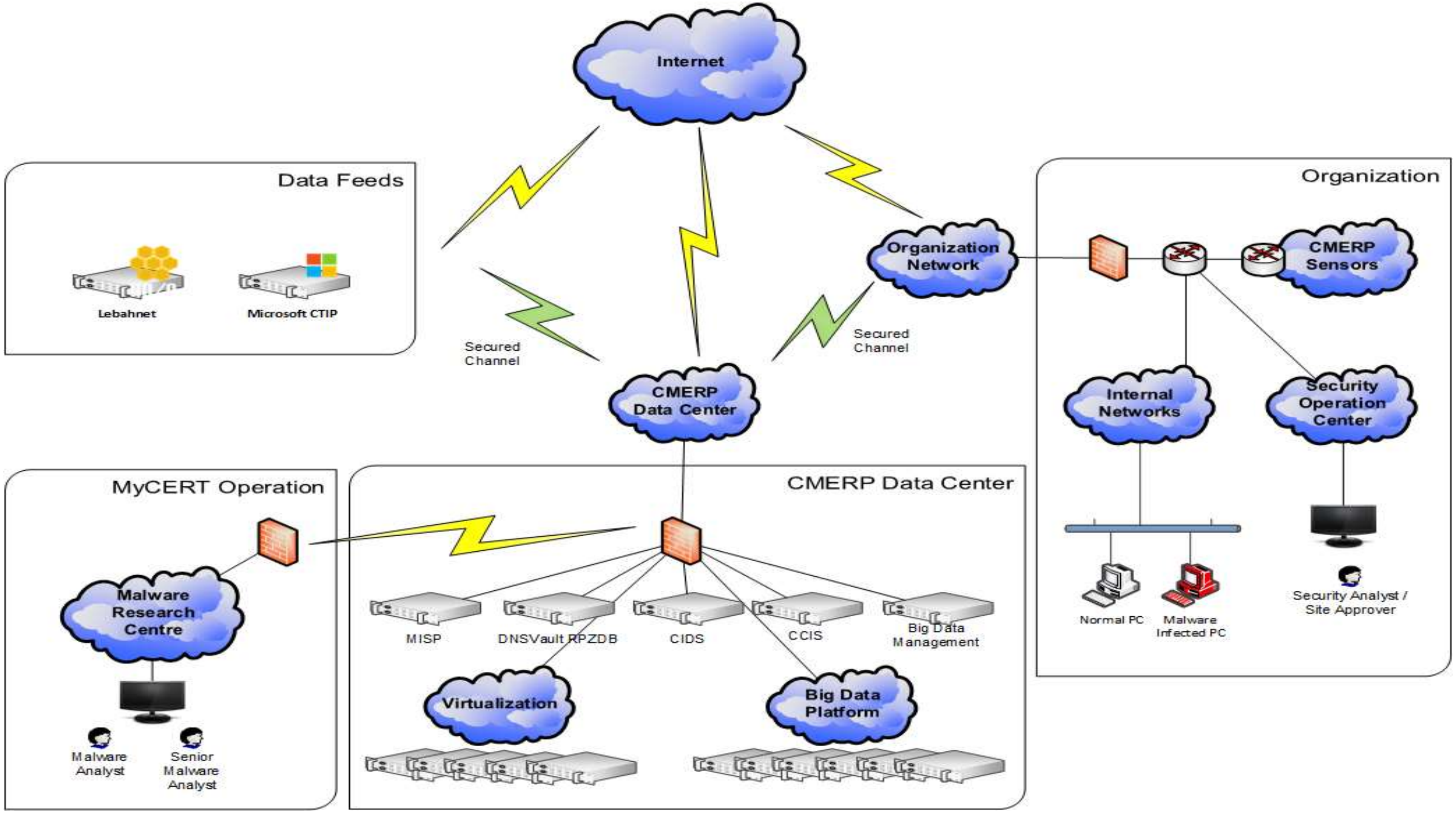
Appropriate removal measures will be given to ensure PC/IP is free from infection.

Back to normal

6

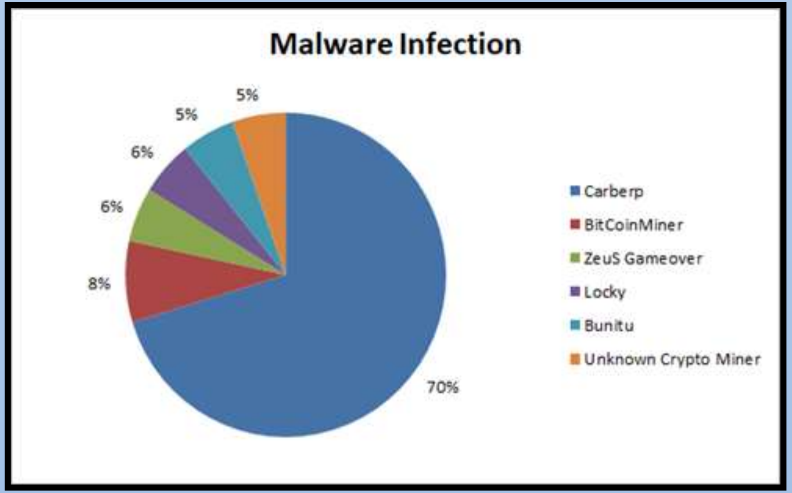
PC/IP was cleaned and regained access to the internet as usual

CMERP Network Infrastructure



Pilot Implementation

Location	: University Campus
Campaign Started	: April 2018
Campaign Ended	: May 2018
Malware Name	: Carberp
Malware Severity	: High

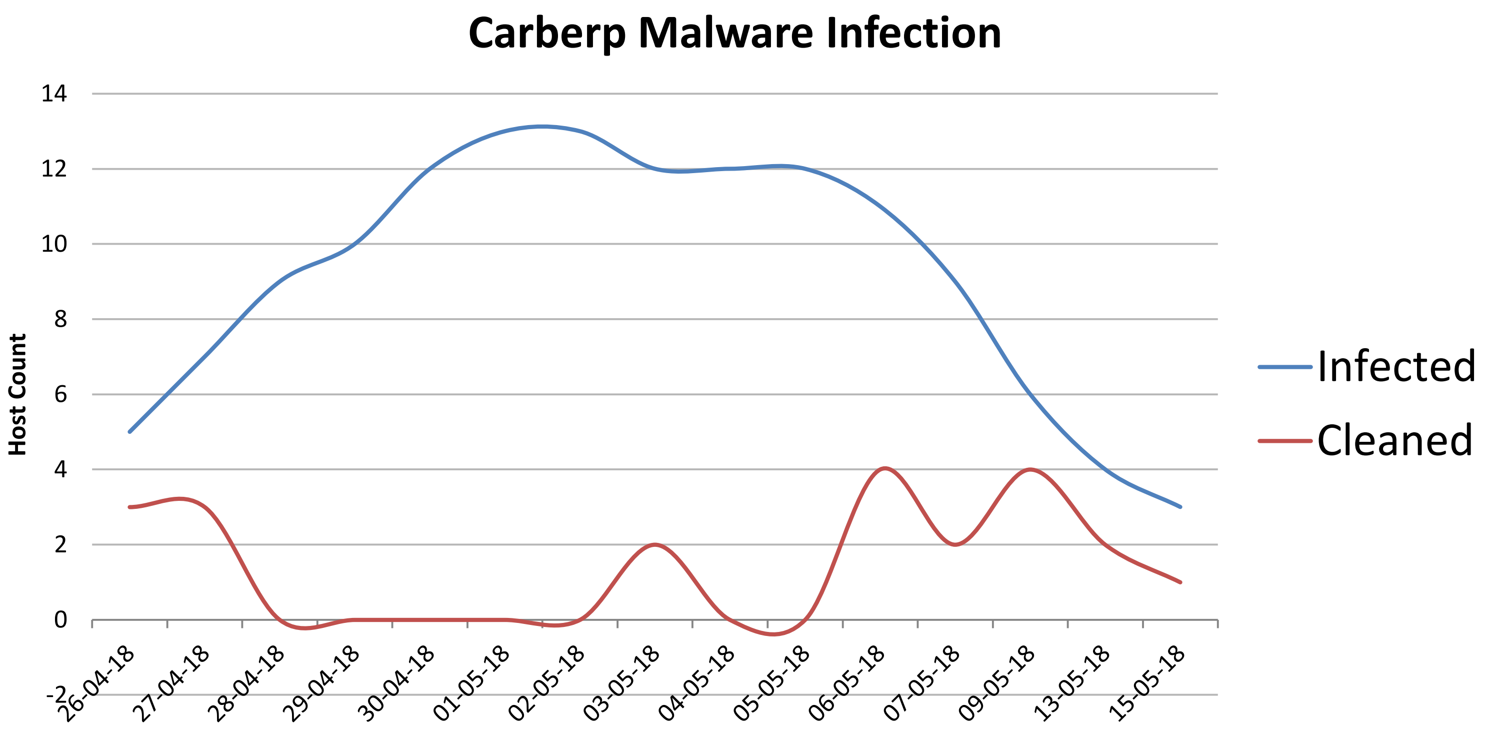


Malware Description:

This family of Trojans can **steal online banking credentials** as well as usernames and passwords from applications. The malware also has the capability to **download other malware** and **steal sensitive information** by taking screenshots or recording keyboard strokes.

Carberp Reference: https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Win32/Carberp

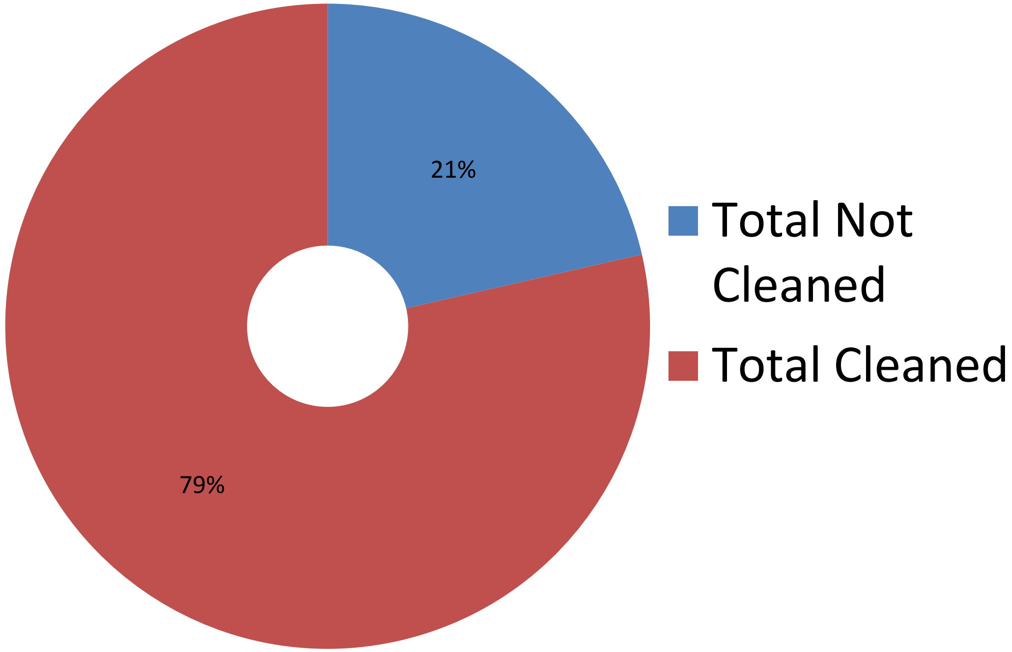
Pilot Outcome



Campaign Management

- •Identified IOC information through malware analysis
- •Redirected all C2 communications through Sinkhole process
- •Infected hosts were quarantine during the Walled Garden process

Pilot Outcome



Analysis of Result:

•Some of Carberp malware variants are not only targeting for Microsoft Windows (PC) but for Android (Mobile Phone); which is outside the scope of this pilot project

•Lack of users awareness on the campaign, thus unable to clean the Carberp malware

Conclusion

1. Our strategy to cope with emerging new threats is by adopting a holistic approach – people, process and technology

2. We need to be prepared all the times by enhancing:
   a. Information sharing amongst relevant stakeholders
   b. Cyber incidents response and coordination
   c. Collaborative & innovative research
   d. Capacity building and education
   e. Acculturation and outreach program

THANKS

2018 ISC 互联网安全大会 中国 · 北京
Internet Security Conference 2018 Beijing · China
（原“中国互联网安全大会”）