



ISC 互联网安全大会



360 互联网安全中心



国家关键信息基础设施应急响应模型

ZAHRI YUNOS

马来西亚CyberSecurity首席运营官

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”)

- 马来西亚通讯和多媒体部下属技术网络安全机构
- 1997年作为马来西亚计算机应急响应团队（MyCERT）开始运作，后来于2007年更名为“CyberSecurity Malaysia”



1997



2001



2005



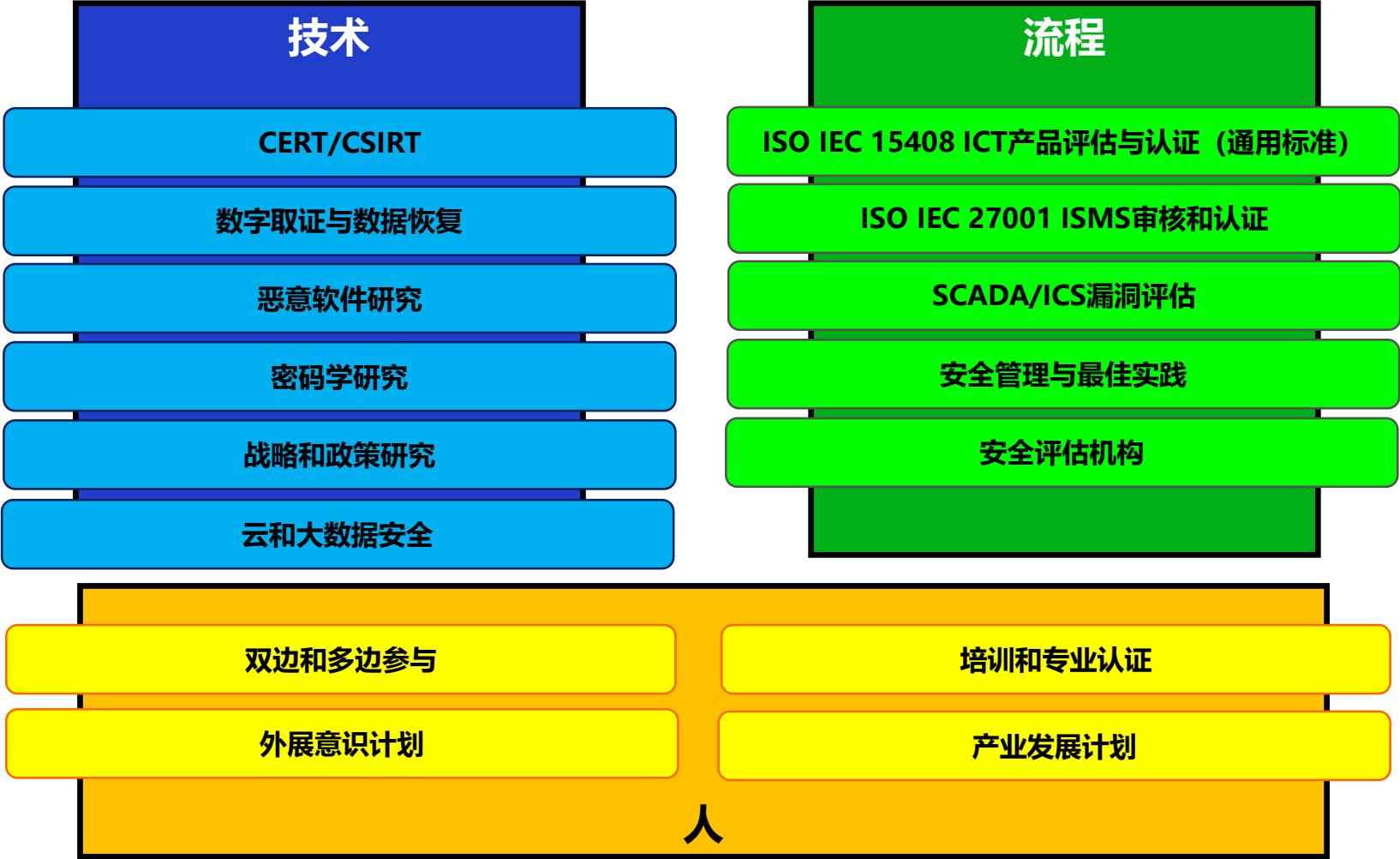
2007



2018

NISER正式注册为“马来西亚网络安全（CSM）”，并隶属于马来西亚科学技术与创新部（MOSTI）。
2007年8月20日，CSM由马来西亚总理创办。

2018年8月，CSM划入马来西亚通讯和多媒体部的管辖范围



保护关键国家信息基础设施 (CNII)

- 对马来西亚电子主权至关重要



CNII:

对国家至关重要的资产、系统和职能部门，如果瘫痪或遭到破坏将会对以下方面产生破坏性影响：

- 国防安全
- 国家经济实力
- 国家形象
- 政府职能
- 公共健康与安全



愿景

“马来西亚的国家关键信息基础设施应该是安全的、可恢复的，同时还是独立的。安全文化的注入会推进社会稳定，增进人民福祉，促进财富创造。”



国防和安全



交通运输



银行与金融



卫生服务



紧急服务

国家关键信息基础设施

对国家至关重要的资产（实物和虚拟）、系统和职能部门，如果瘫痪或遭到破坏将会对以下方面产生破坏性影响

- 国防安全
- 国家经济实力
- 国家形象
- 政府职能
- 公共健康与安全



能源



信息和通讯



政府

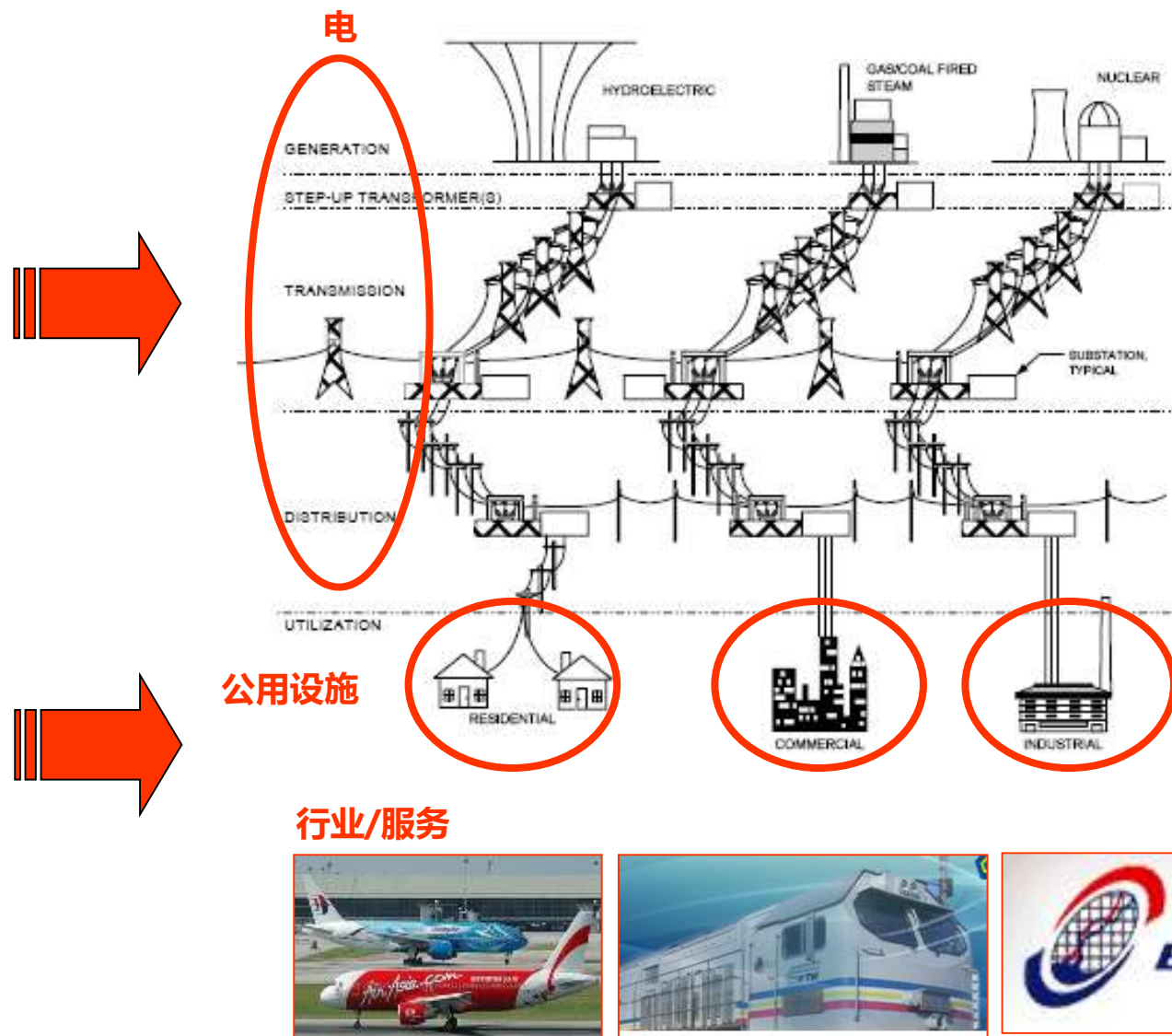


食品与农业

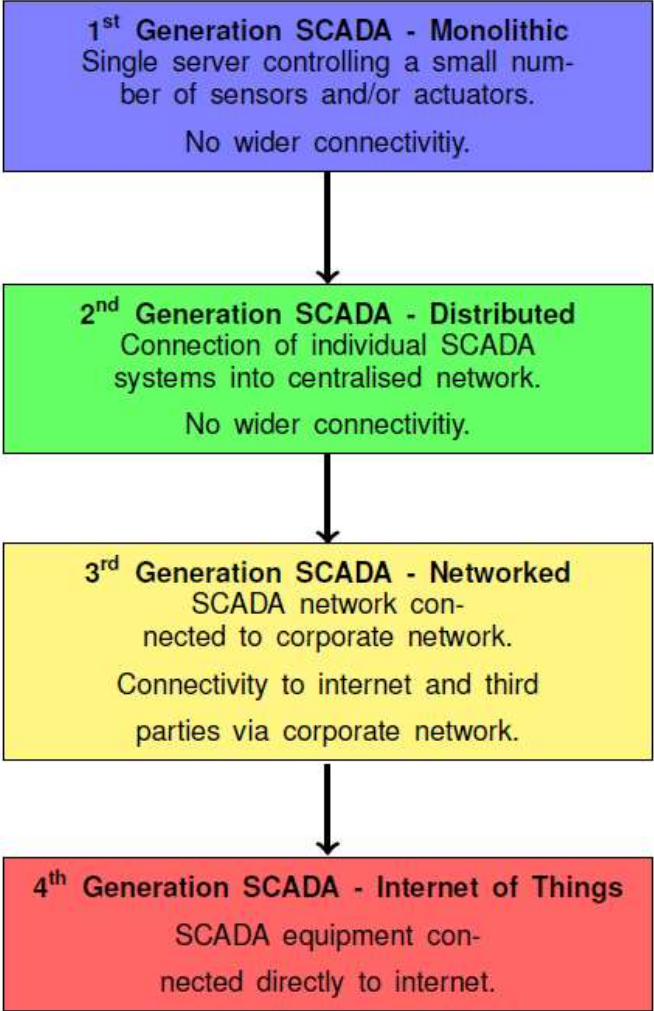
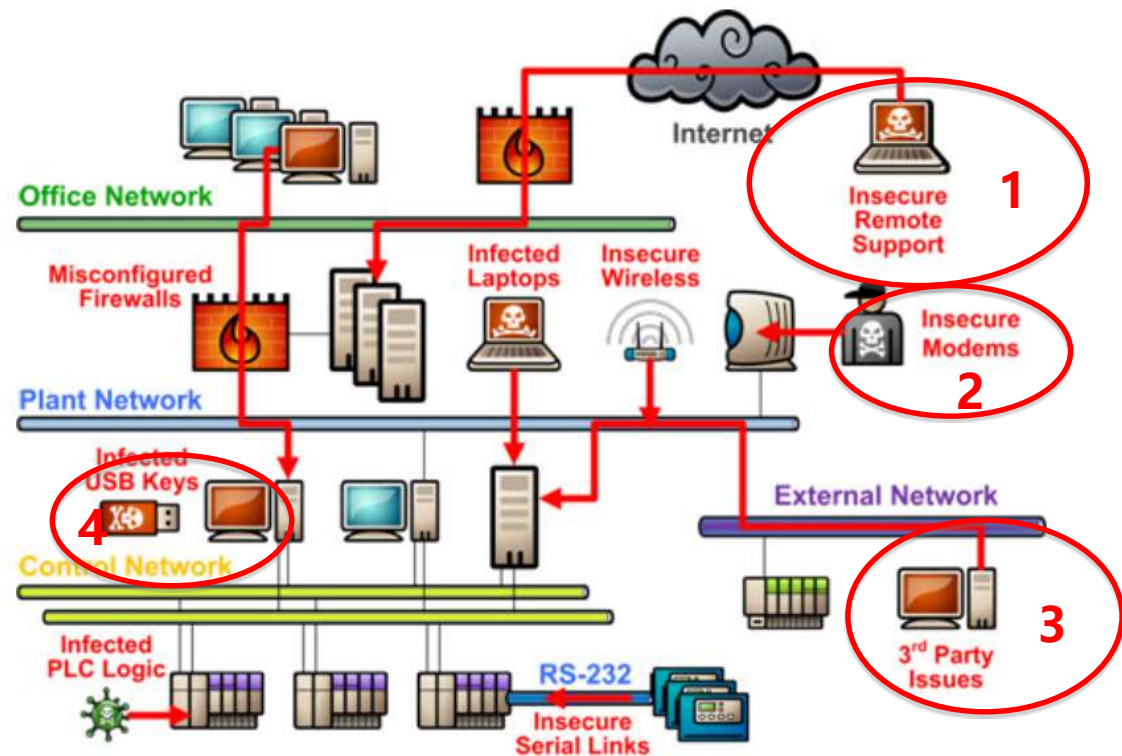


水

关键信息基础设施
的高度依赖意味着
一个领域出现故障
将会波及其他领域。



SCADA = 监视控制与数据采集



对CNII的威胁：恐怖分子利用ICT和网络空间





技术相关威胁

黑客威胁



入侵



欺诈



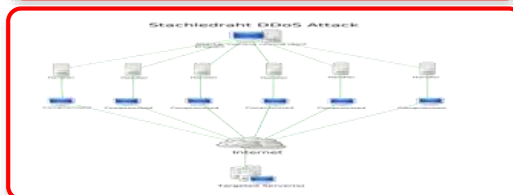
垃圾邮件



恶意代码



拒绝服务攻击



网络内容相关威胁

国家安全威胁



网络骚扰



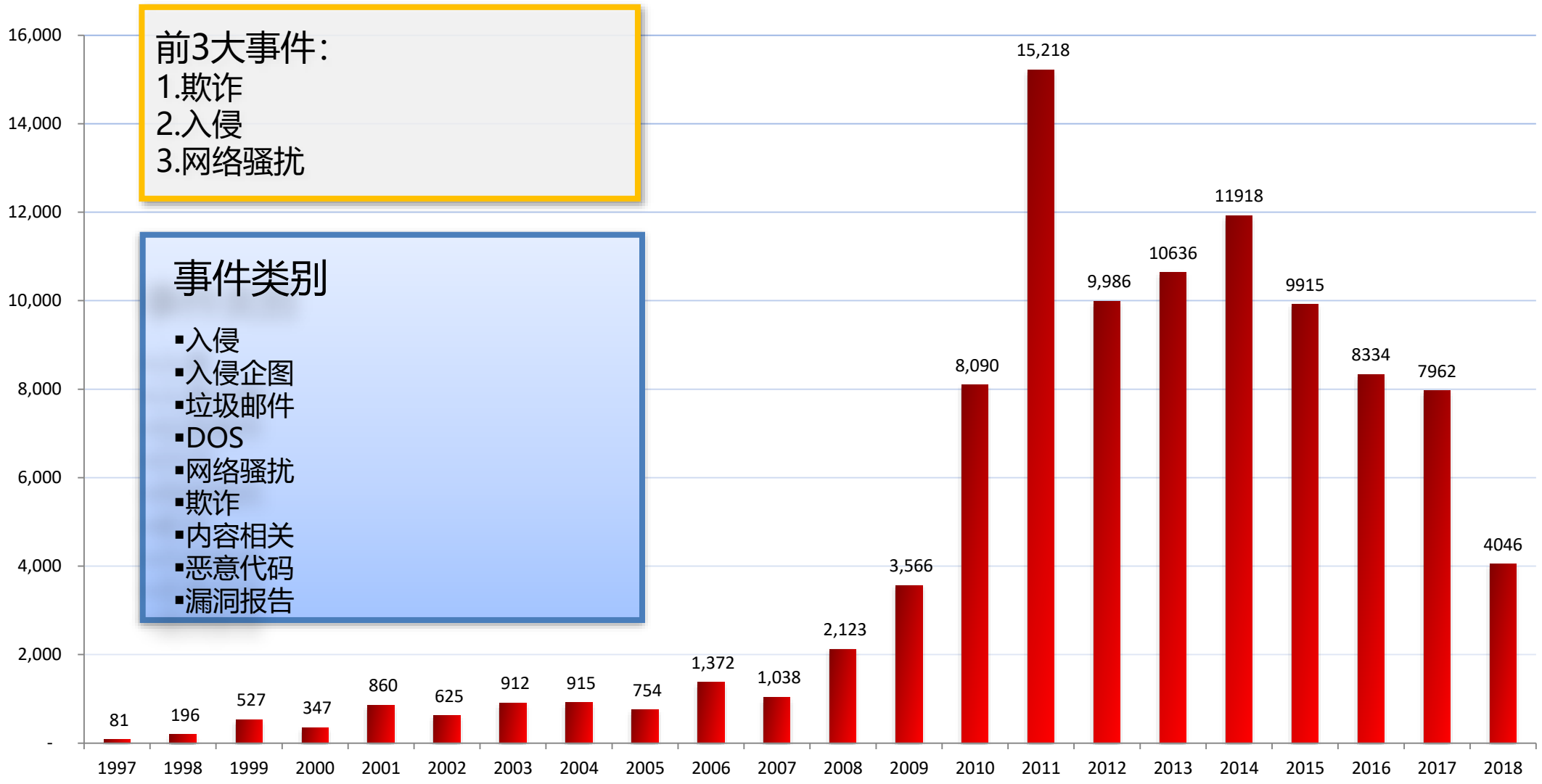
儿童色情



虚假新闻/诽谤

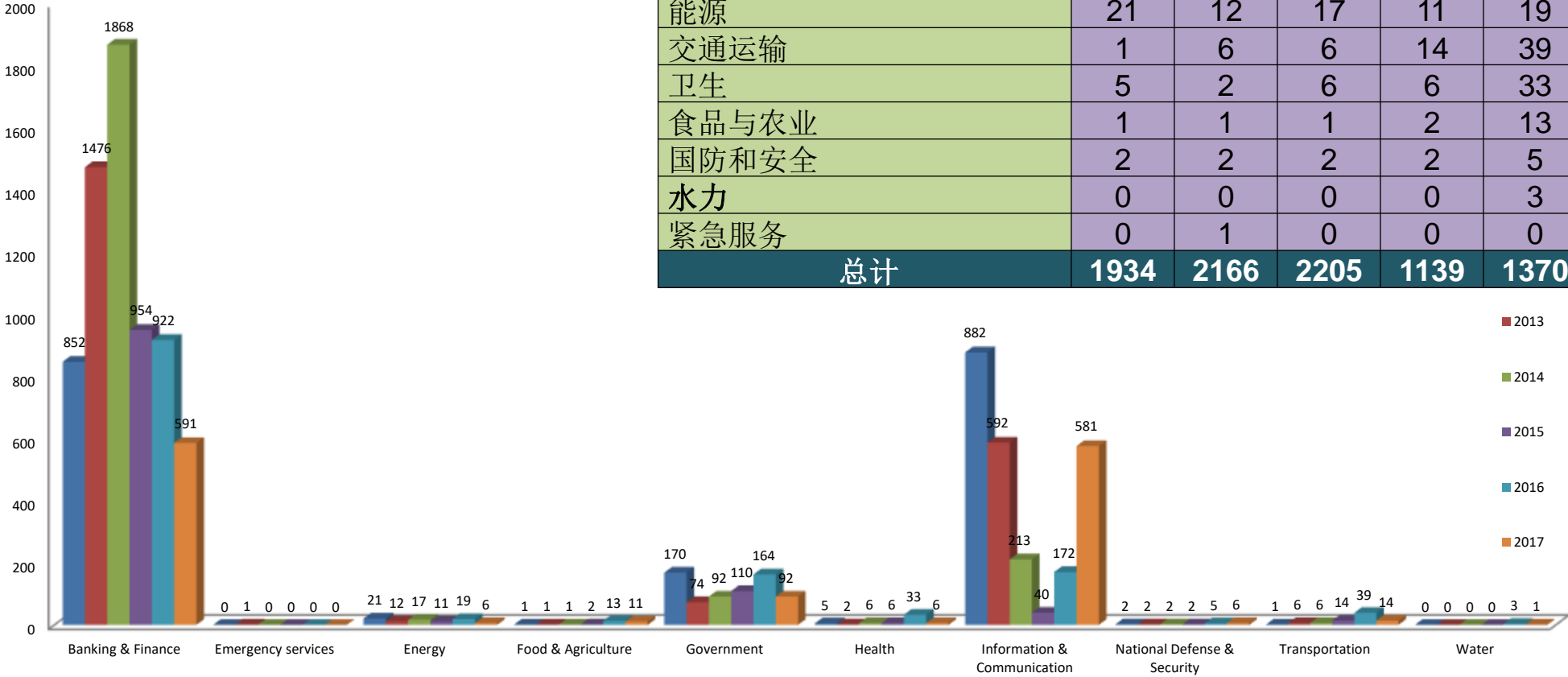






按行业划分的网络事件 (2012-2017)

资料来源: www.mycert.org.my



	2012	2013	2014	2015	2016	2017	总计
银行与金融	852	1476	1868	954	922	591	6663
信息与通信	882	592	213	40	172	581	2480
政府	170	74	92	110	164	92	702
能源	21	12	17	11	19	6	86
交通运输	1	6	6	14	39	14	80
卫生	5	2	6	6	33	6	58
食品与农业	1	1	1	2	13	11	29
国防和安全	2	2	2	2	5	6	19
水力	0	0	0	0	3	1	4
紧急服务	0	1	0	0	0	0	1
总计	1934	2166	2205	1139	1370	1308	10122

1) 法律挑战

通报网络事件不是强制性的

跨境管辖权

身份识别/所有权

2) 技术挑战

反取证技术

匿名技术

物联网技术

3) 监管挑战

互联互通关系

预算和资金

联合组织/有组织的网络犯罪



愿景

马来西亚的**国家关键信息基础设施**应该是安全、可恢复的，同时还是独立的。安全文化的注入会推进社会稳定，增进人民福祉，促进财富创造

目标

- 应对**国家关键信息基础设施 (CNII)** 面临的风险
- 确保关键基础设施受到保护，且保护力度与安全风险**相一致**
- 明确并制定**全面的计划和一系列**安全**框架



通过公共和私人合作与协调，为马来西亚CNII制定出缓解和应对网络攻击的策略框架



练习目标:

- 1.检查有效性，找出差距并改进NCCMP的沟通程序、响应能力和协调性
- 2.了解CNII机构的网络事件处理机制
- 3.了解CNII机构在网络事件发生期间的沟通。

2013年，马来西亚国家安全委员会（NSC）发布了指导方针“NSC指令24：国家网络危机管理机制。”

该指令规定，各政府机构应建立自己的CSIRT作为管理网络事件的一个举措

2013年，最新版本的ISMS标准（27001：2013（E））在A16.1段中附加了三个子条款，强调对信息安全事件的响应和评估：

1. A 16.1.5 对信息安全事件的响应
2. A 16.1.6 从信息安全事件中学习
3. A 16.1.7 证据收集

1.我们的服务: CyberDEF



D

“检测网络威胁”

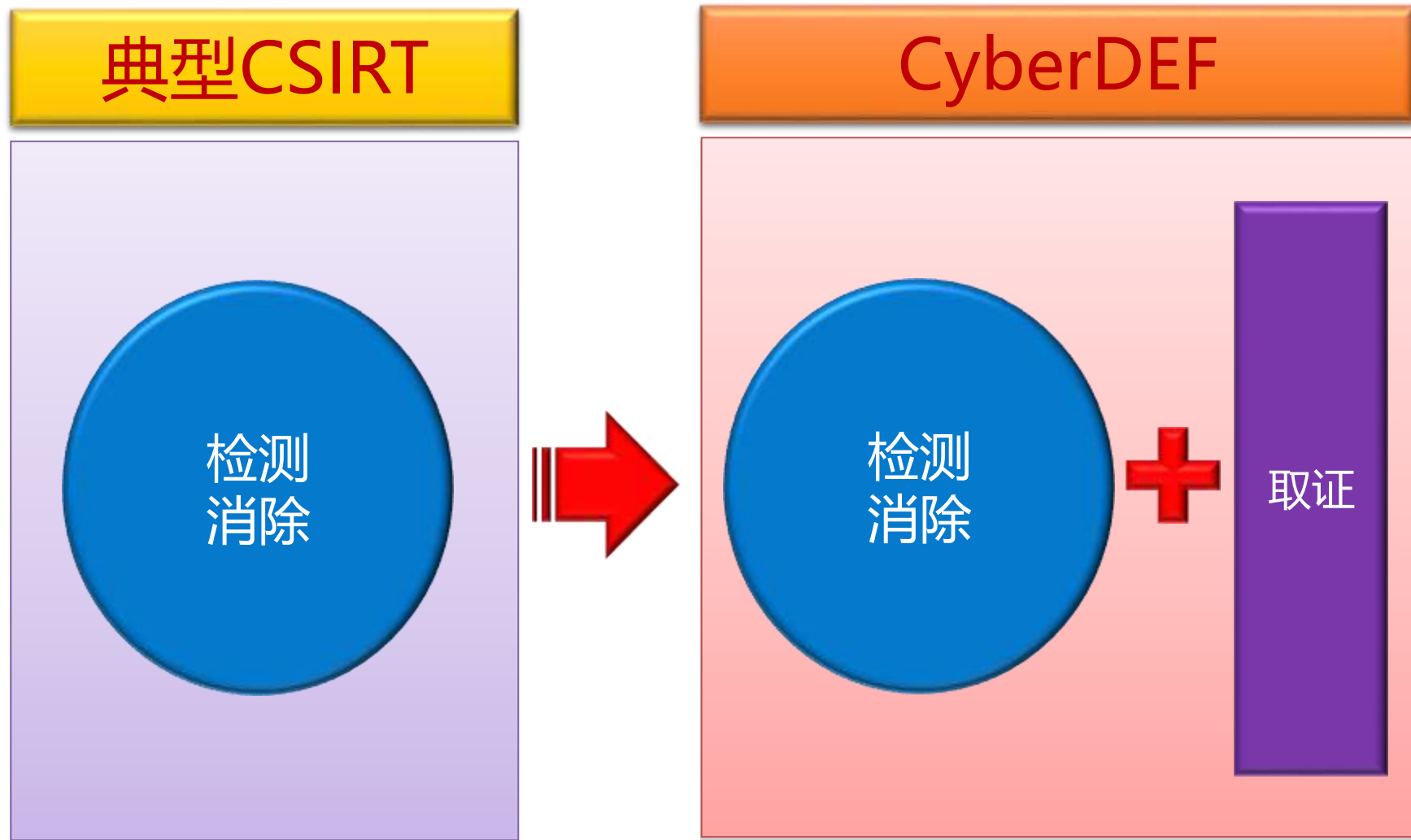
E

“消除网络威胁”

F

“网络威胁的取证分析”

此阶段可迭代, 返回
“D” 或 “E” 进一步
改进技术



检测

识别任何漏洞、缺陷和现有威胁

1. 传感器
2. 沙箱
3. 分析
4. 可视化

消除

修复漏洞、修补缺陷并应对现有威胁

开展网络威胁演习或演练，以测试新型防御/预防系统的可行性与灵活性

取证

1. 电子取证
2. 根本原因分析
3. 调查
4. 取证准备
5. 取证合规



为何网络防御与众不同？

3 技术部门

由 3个技术部门组成：

1. 安全技术服务部门 (STS)
2. 数字取证部门 (DF)
3. 马来西亚计算机应急响应小组 (MyCERT)

集中 管制

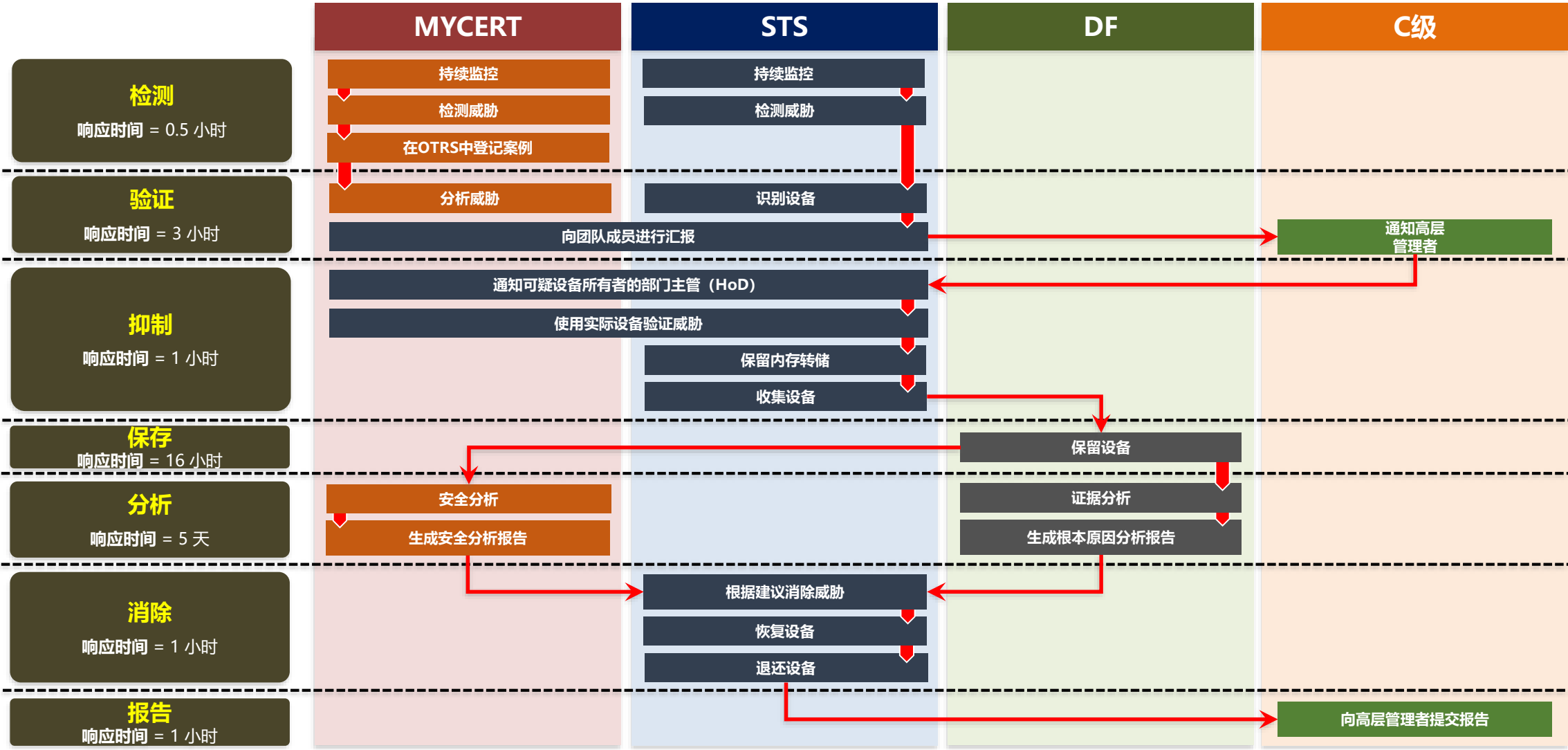
有效的**集中管制**，因为所有3个部门都归属于网络安全响应服务部门

取证 元素

取证元素**包含**在提供的服务中



计算机安全事件响应小组（CSIRT）的管理工作流程



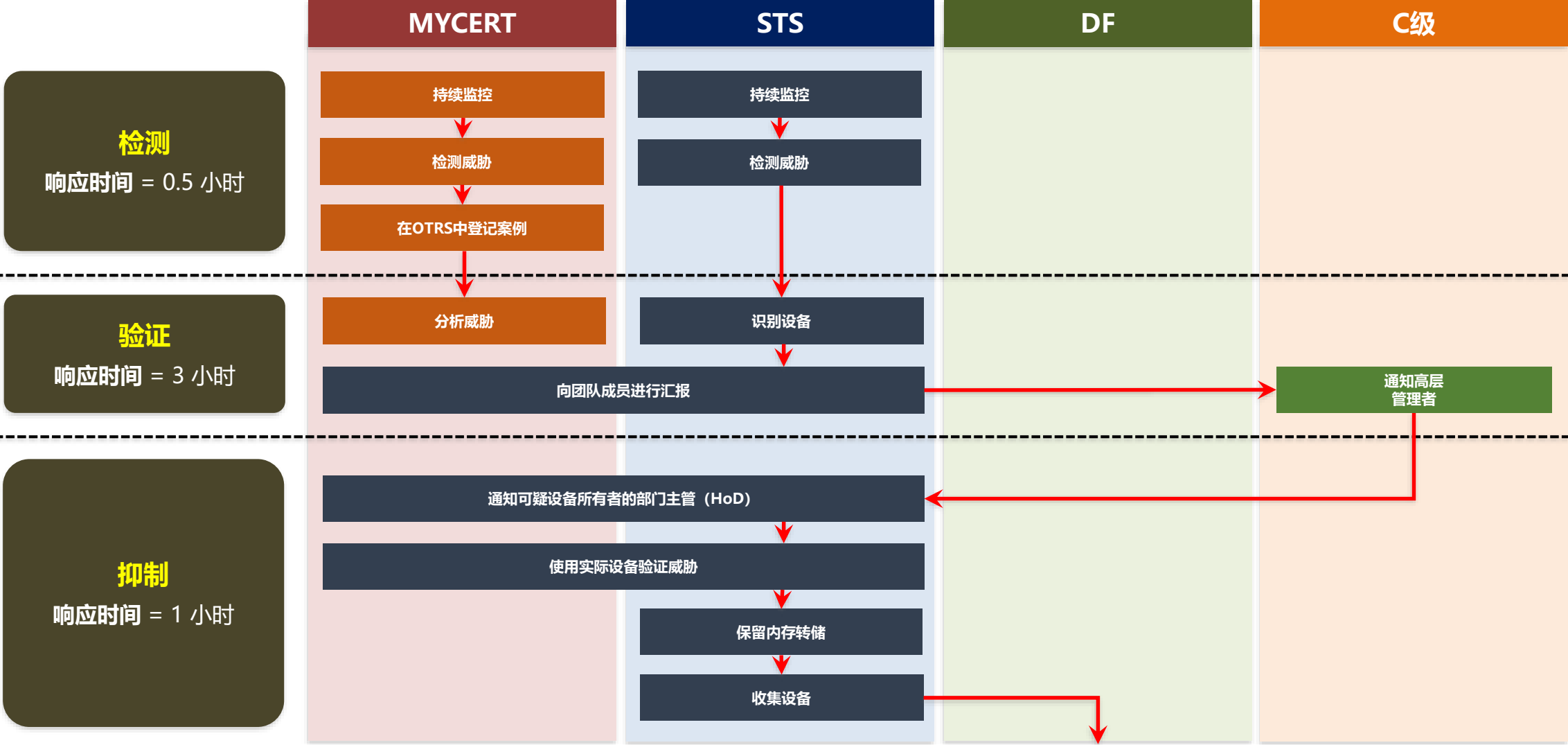
计算机安全事件响应小组（CSIRT）的管理工作流程



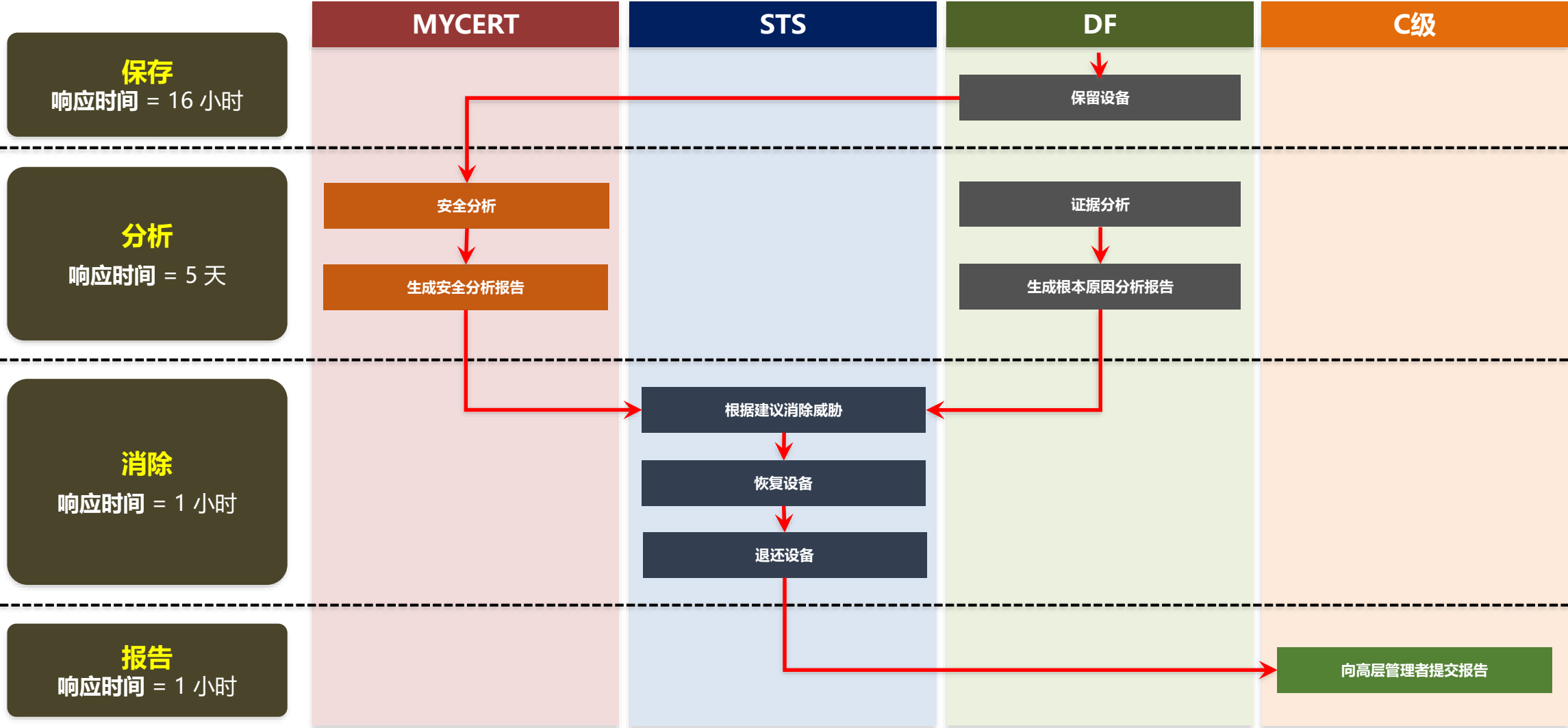
ISC 互联网安全大会

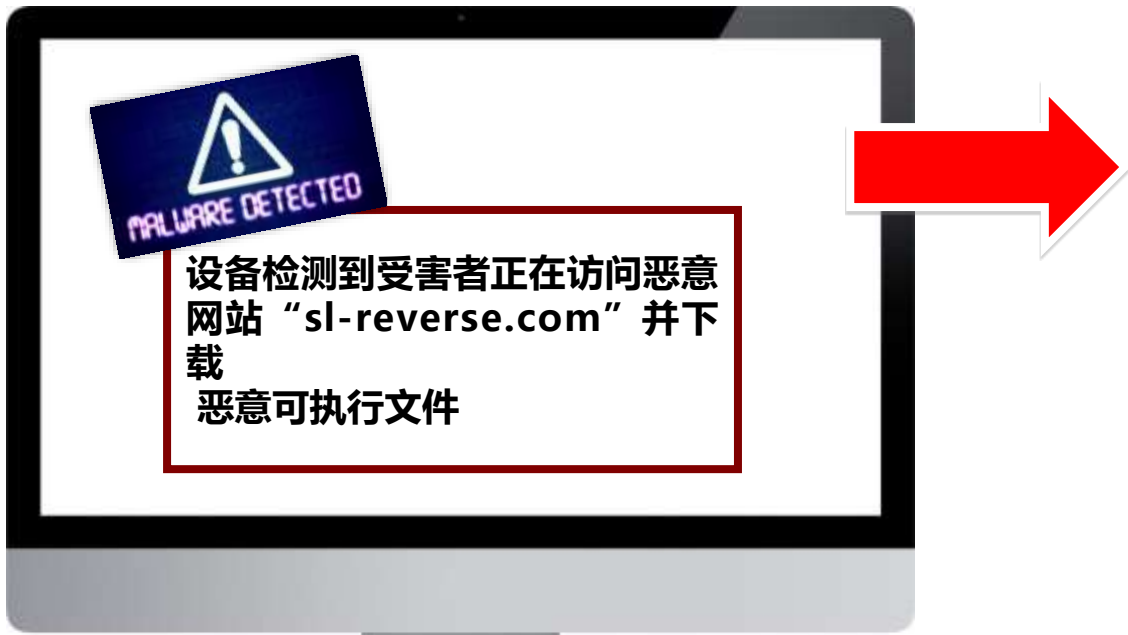


360 互联网安全中心



计算机安全事件响应小组（CSIRT）的管理工作流程





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 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

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

确定受影响的设备

IP Address	xx.x.xx.xxx
MAC Address	xc:0x:x1:xf:52:ex
NetBIOS Name	[REDACTED]
Staff Name	[REDACTED]
Location	[REDACTED] (WVDP)
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

消除恶意软件

- 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.

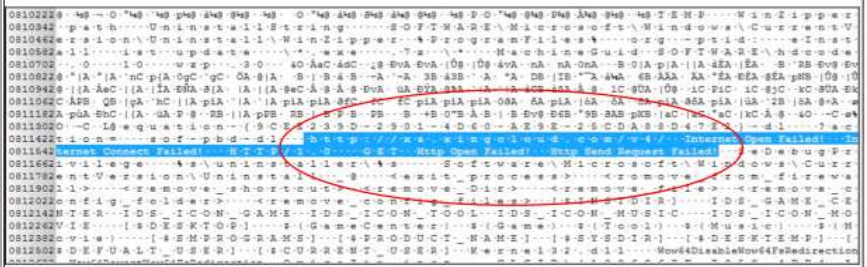
分析

从恶意文件中提取出元数据和注册表信息，并进行取证分析

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

发现

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



Screenshot 2: wzUpd.exe access to several URLs

Screenshot 3: wzUpg.exe application run count

2.我们的服务：CMERP 协同恶意软件根除与修复项目

目标：减少马来西亚感染恶意软件的数量



收集

- 检测
- 标准化
- 丰富化
- 相关性



分析

- 静态
- 动态
- C2识别



识别

- 恶意域名识别
- 恶意IP 识别
- 受感染的主机识别



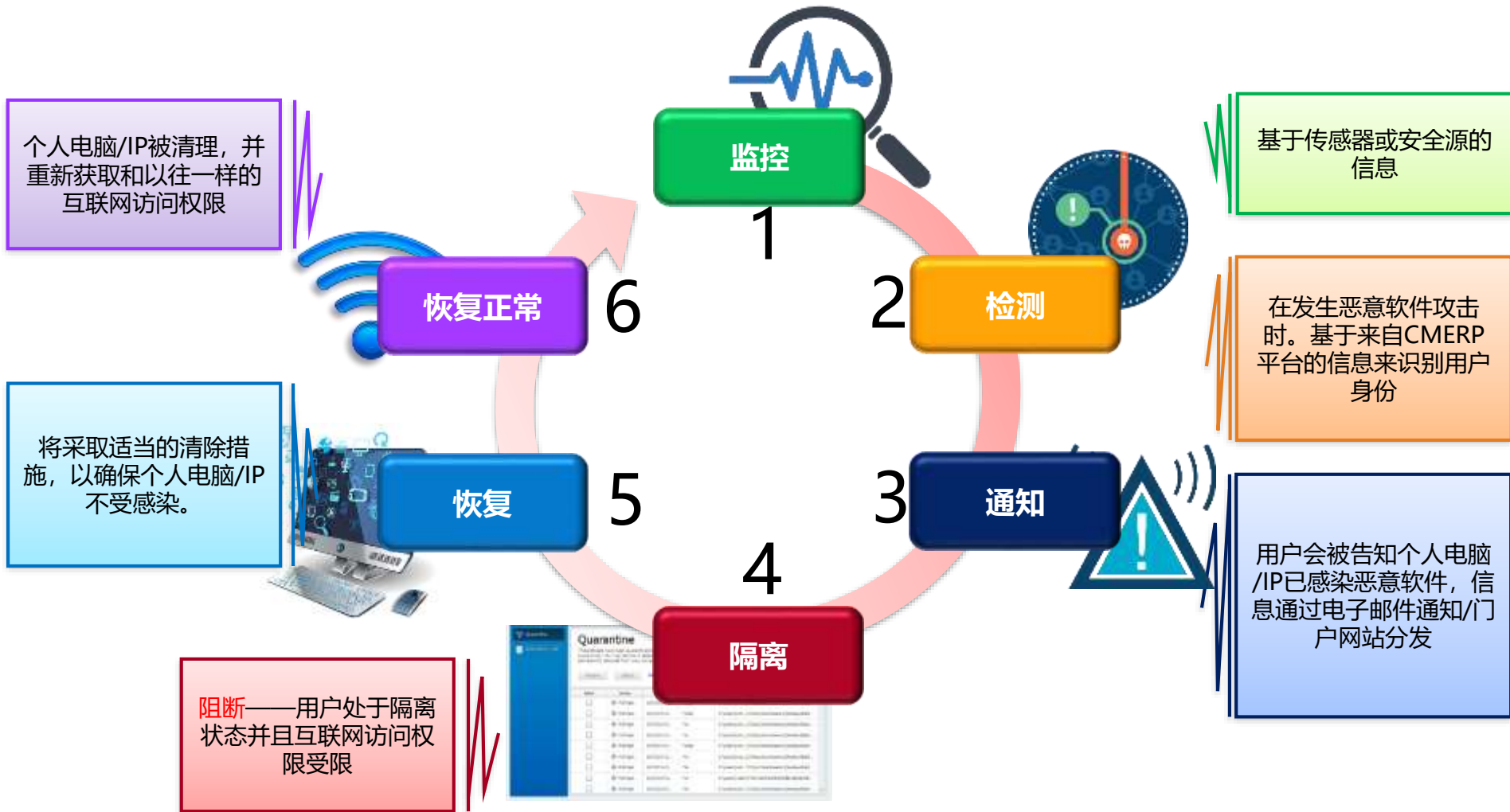
阻断

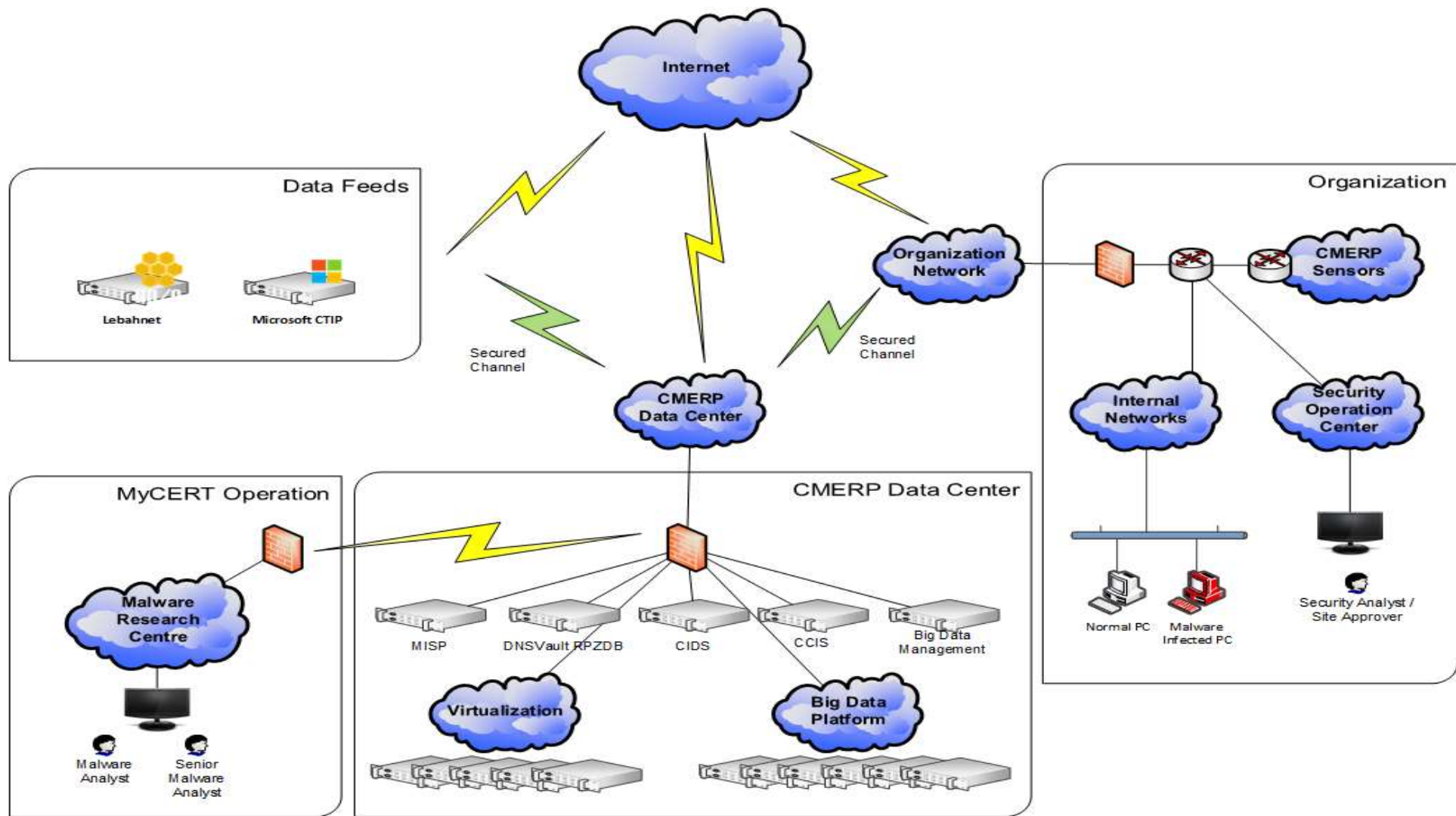
- 抑制
- 恶意软件清除/根除



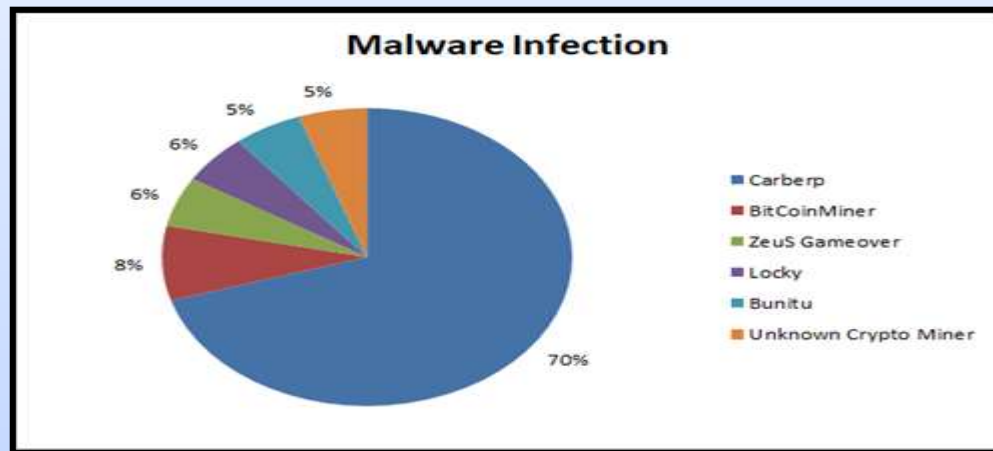
报告

- 统计
- 对比
- 趋势





位置 : 大学校园
活动开始于 : 2018年4月
活动结束于 : 2018年5月
恶意软件名称 : Carberp
恶意软件严重性 : 高

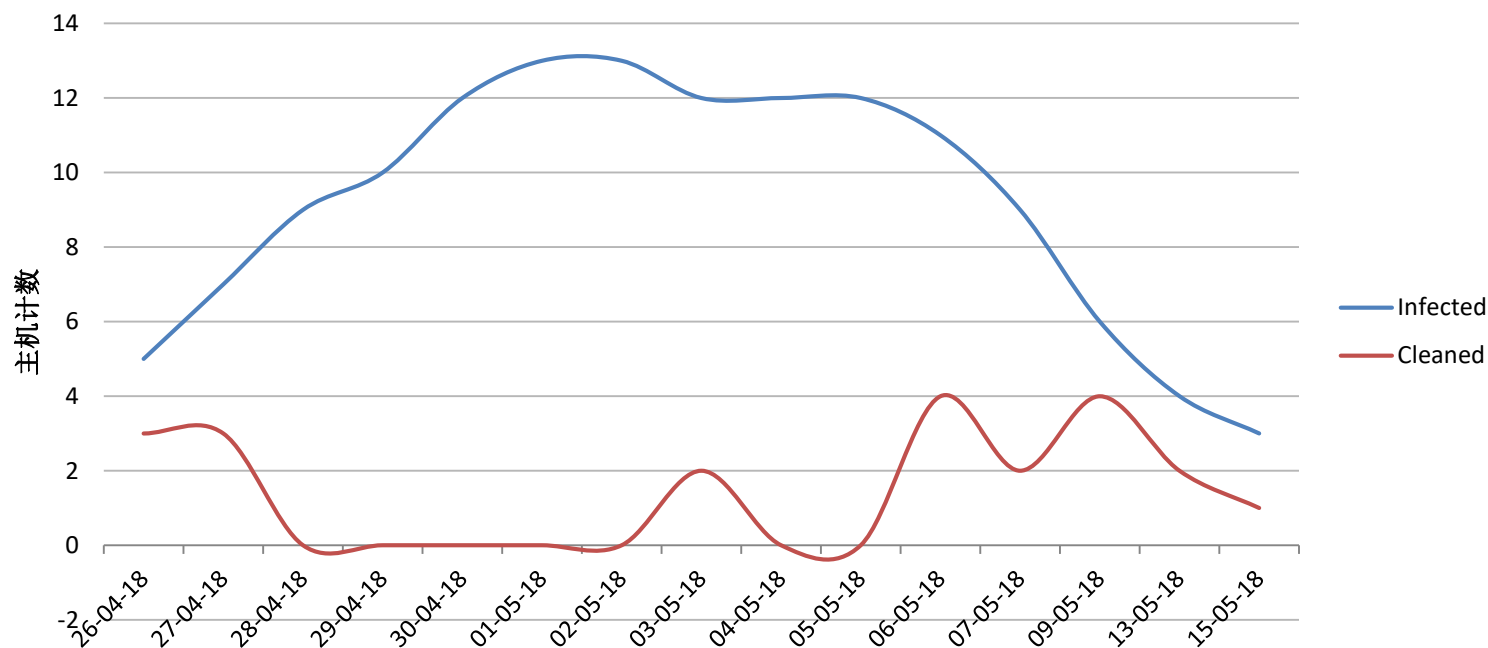


恶意软件描述:

此类木马可以从应用程序中窃取网上银行凭证以及用户名和密码。该恶意软件还具有下载其它恶意软件, 并通过屏幕截图或记录键盘敲击来窃取敏感信息的能力。

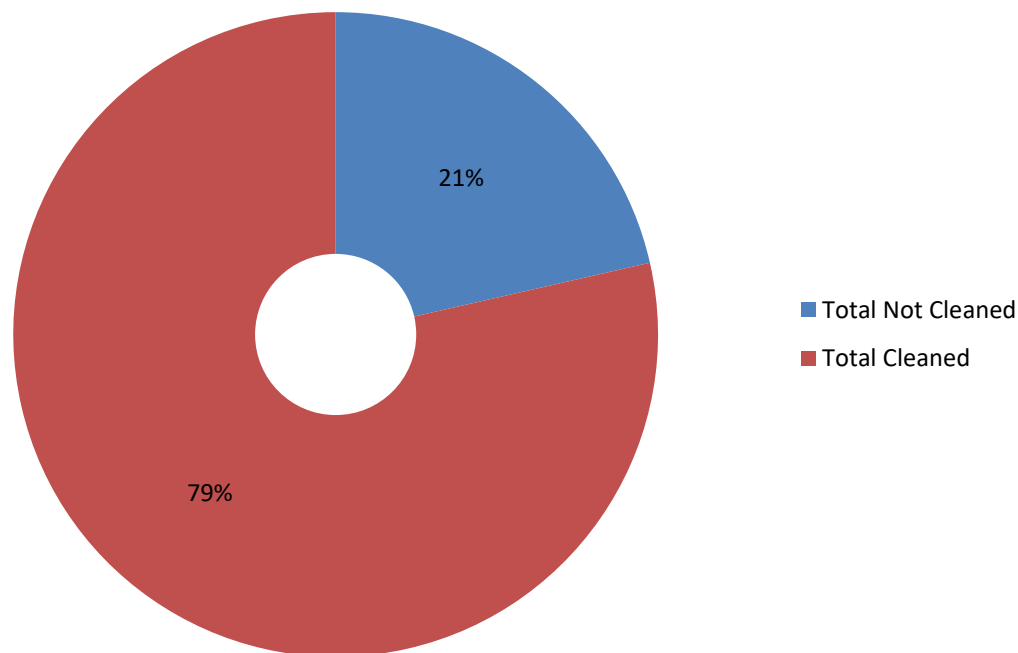
Carberp参考: <https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Win32/Carberp>

Carberp恶意软件感染



活动管理

- 通过对恶意软件分析识别出受损的迹象（IOC）信息
- 通过匹配过程重定向所有C2通信
- 在阻断过程中隔离受感染的主机



结果分析:

- 一些Carberp恶意软件变种不仅针对微软Windows（个人电脑），也针对Android（移动电话）；这超出了该试点项目的范围
- 用户缺乏对此活动的认知，因此无法清除Carberp恶意软件

1. 我们对出现的新型威胁的应对策略是采用整体分析——人员、流程和技术
2. 我们需要通过加强以下几点，时刻做好准备
 - a. 相关干系人之间的信息共享
 - b. 网络事件的响应与协调
 - c. 协作和创新研究
 - d. 能力建设与教育
 - e. 文化适应与外展计划



ISC 互联网安全大会



360 互联网安全中心

谢谢!

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”)