

SOC的進度及資安通報統計

中央大學 電算中心

呂芳發

2011-04-19

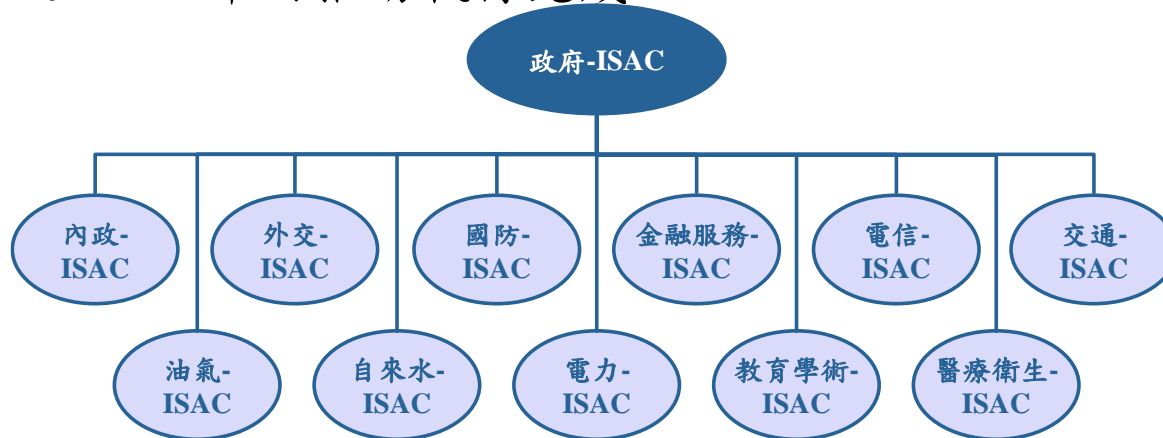


大 網

- ☐ 北區A-SOC 計畫建置SOC的進度
- ☐ 資安通報統計

緣起

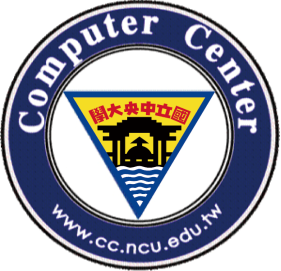
- 教育部為配合行政院國家資通安全會報建立政府資通安全防護管理中心功能，規劃建置「教育學術資安資訊分享與分析中心(A-ISAC)」平台，為教育部所屬台灣學術網路(Taiwan Academic Network, TANet)連線之各級學校提供資安防護與資訊分享機制。
- 教育部規劃逐步建立教育體系特色之資安資訊交換及分析防護機制，並於四年內推動執行完成。





計畫目標

- ☐ 建置北區A-SOC資訊安全監控環境
- ☐ 強化北區A-SOC資訊安全防護機制
- ☐ 建立北區A-SOC資訊安全警訊通報機制
- ☐ 建立學術網路資安追蹤與鑑識機制(示範點)
- ☐ 簡化區網中心監控點資訊安全管理制度
- ☐ 培訓資安專業分析人員



SOC 中心五大主要功能

□ 事前預防

- 資安警訊管理
- 資安弱點管理

□ 事中監看

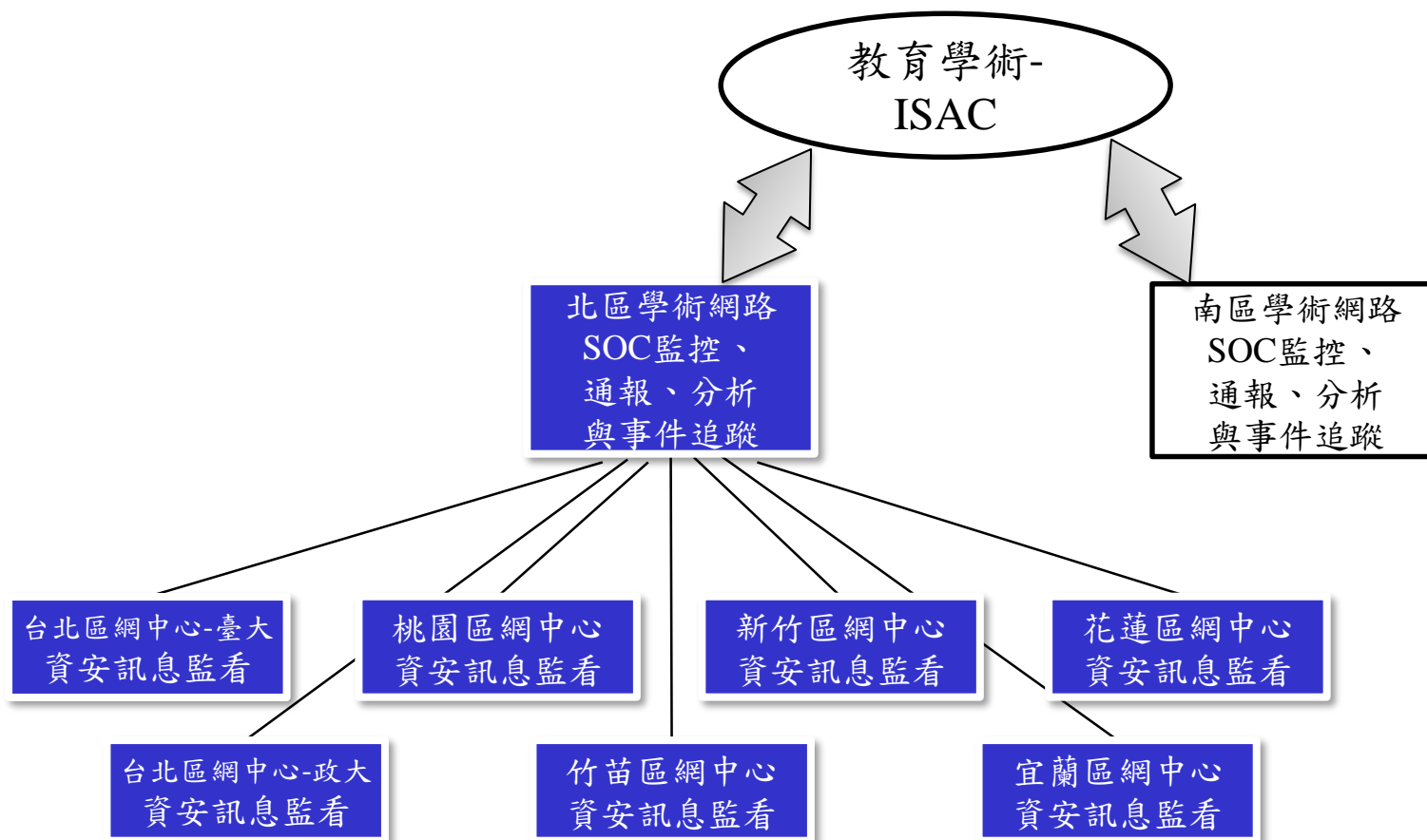
- 資安設備管理
- 資安事件監看

□ 事後處理

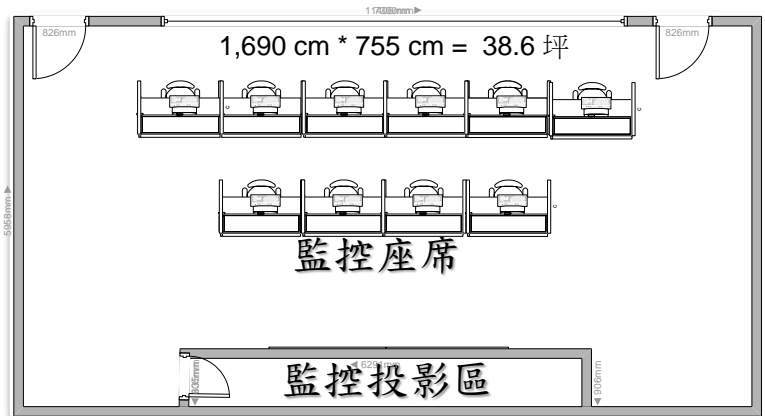
- 資安事故處理



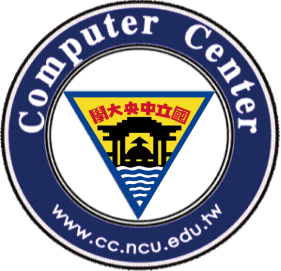
教育學術資訊事件分析與分享架構



學術網路資訊安全監控中心



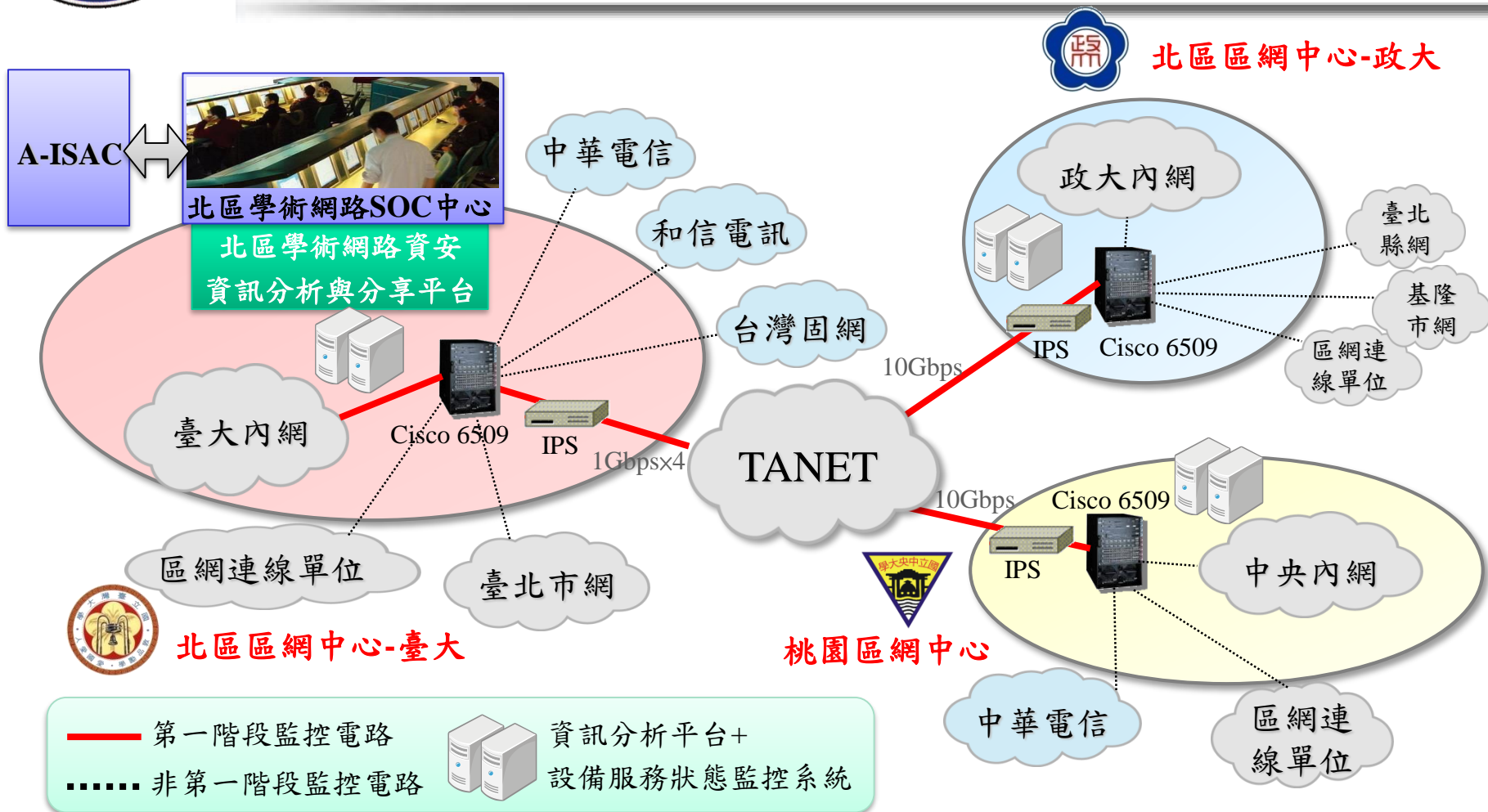
- 建置於臺大計算機及資訊網路中心
- 負責北區學術網路資安訊息監控、收集、分析、通報以及處理作業
- 規劃一、二、三線監控人員
 - 一線 7×24 監控與通報
 - 二、三線 5×8 系統維運、事件分析、事件處理



強化北區A-SOC資訊安全防護機制

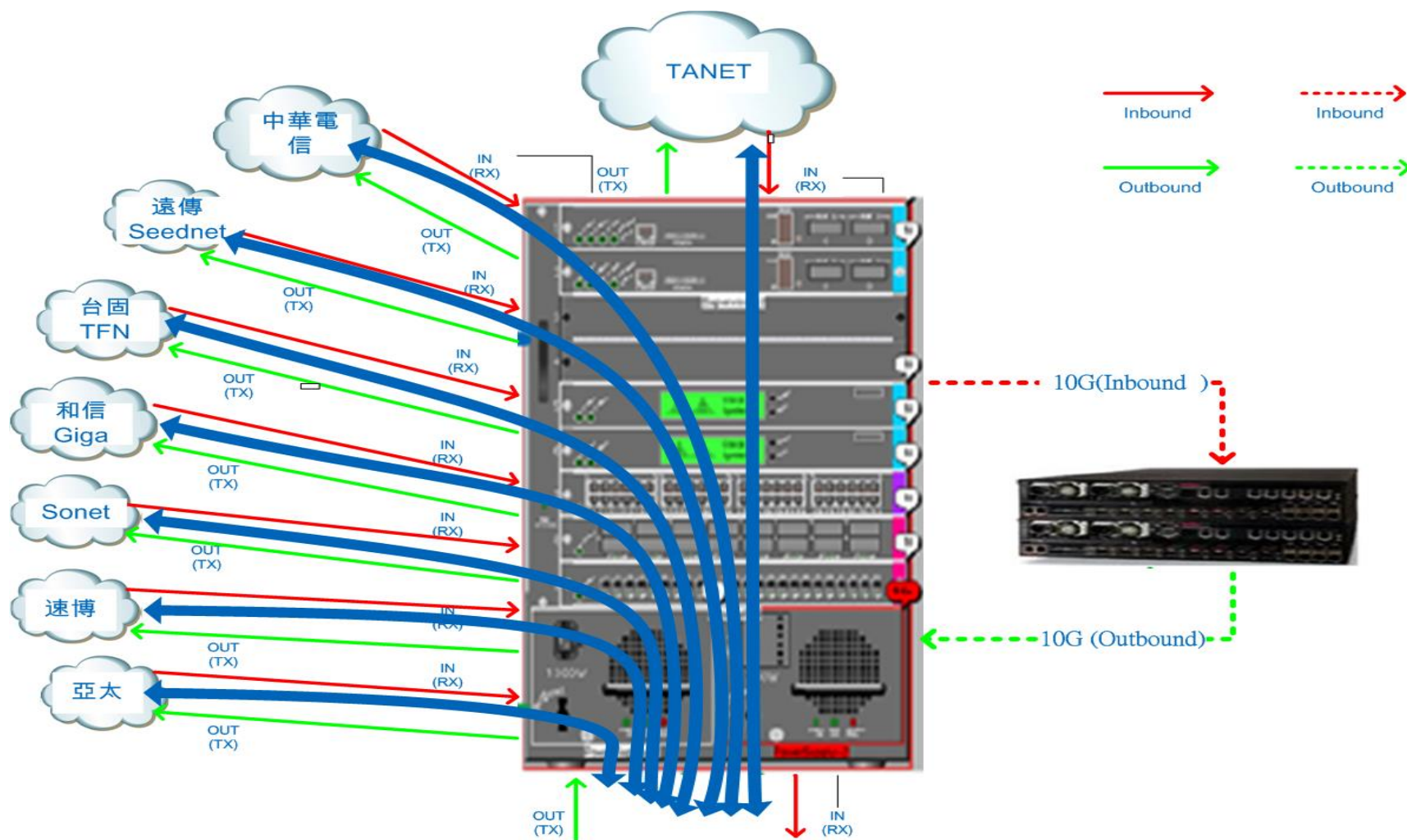
- 部署入侵防禦設備
 - 可配合緊急應變機制即時阻擋惡意連線
- 建置設備服務狀態系統
 - 監控各監控點區網中心之網路設備與資安設備
- 建置資訊分析平台
 - 收集各監控點資安事件，進行初步關聯性分析

資安監控點佈署規劃



桃園區網IPS架構

□ 99/11數聯資安得標,99/12/31上線





Real Time Monitor

Real-time Threat Analyzer

Server Name: 192.192.227.23 | User: LU | Domain: /NCU

McAfee®
Network Security Manager
Threat Analyzer

Dashboards Alerts Hosts Incident Viewer Host Forensics Preferences

All Alerts Display Filter

/ All Alerts Detail Group By Admin Domain

1	Time	Attack Name	Dest Port	Result	Category
	04/19 15:24:24	L HTTP: Response UTF16/32 Encoding	52016	Maybe Successful	Exploit
	04/19 15:24:24	M UDP: Host Sweep	53	Suspicious	Reconnaissance
	04/19 15:24:23	M TCP: ACK Port Scan	0	Suspicious	Reconnaissance
	04/19 15:24:21	M HTTP: Thtpd Stack Overflow	80	Maybe Successful	Exploit
	04/19 15:24:21	M UDP: Host Sweep	53	Suspicious	Reconnaissance
	04/19 15:24:21	M UDP: Host Sweep	17788	Suspicious	Reconnaissance
	04/19 15:24:20	M TCP: ACK Port Scan	0	Suspicious	Reconnaissance
	04/19 15:24:20	M UDP: Host Sweep	53	Suspicious	Reconnaissance
	04/19 15:24:19	M TCP: Full-Connect Host Sweep	80	Suspicious	Reconnaissance
	04/19 15:24:19	M HTTP: QQzone User Login Detected	80	Suspicious	Policy Violation
	04/19 15:24:19	M DNS: Microsoft Windows Internet Connection Sharing ...	0	Maybe Successful	Exploit
	04/19 15:24:19	M DNS: Microsoft Windows Internet Connection Sharing ...	0	Maybe Successful	Exploit
	04/19 15:24:17	M TCP: ACK Port Scan	0	Suspicious	Reconnaissance
	04/19 15:24:17	L SCAN: SYN FIN Based Probes	0	Suspicious	Exploit
	04/19 15:24:17	M TCP: ACK Port Scan	0	Suspicious	Reconnaissance
	04/19 15:24:16	M SMTP: Mail Relay Attempt	0	Maybe Successful	Policy Violation
	04/19 15:24:15	M TCP: SYN Host Sweep	21	Suspicious	Reconnaissance
	04/19 15:24:15	RED BOT: IRC SCAN Activity	1097	Blocked	Malware
	04/19 15:24:15	M TCP: SYN Host Sweep	22	Suspicious	Reconnaissance
	04/19 15:24:14	M TCP: ACK Port Scan	0	Suspicious	Reconnaissance
	04/19 15:24:09	M TCP: Full-Connect Host Sweep	80	Suspicious	Reconnaissance
	04/19 15:24:09	M UDP: Port Scan	0	Suspicious	Reconnaissance
	04/19 15:24:09	L HTTP: Response UTF16/32 Encoding	12564	Maybe Successful	Exploit
	04/19 15:24:08	M TCP: ACK Port Scan	0	Suspicious	Reconnaissance
	04/19 15:24:07	M ICMP: Destination Unreachable DOS	0	Maybe Successful	Exploit
	04/19 15:24:07	RED NETBIOS-SS: Microsoft Server Service Remote Code E...	0	Maybe Successful	Exploit
	04/19 15:24:05	M HTTP: Windows Media ASX PlayList Vulnerability	4531	Maybe Successful	Exploit
	04/19 15:24:05	M TCP: ACK Host Sweep	80	Suspicious	Reconnaissance

Total Rows 20605

Search Alert Save as CSV Save as PDF Save View Saved Views Quarantine

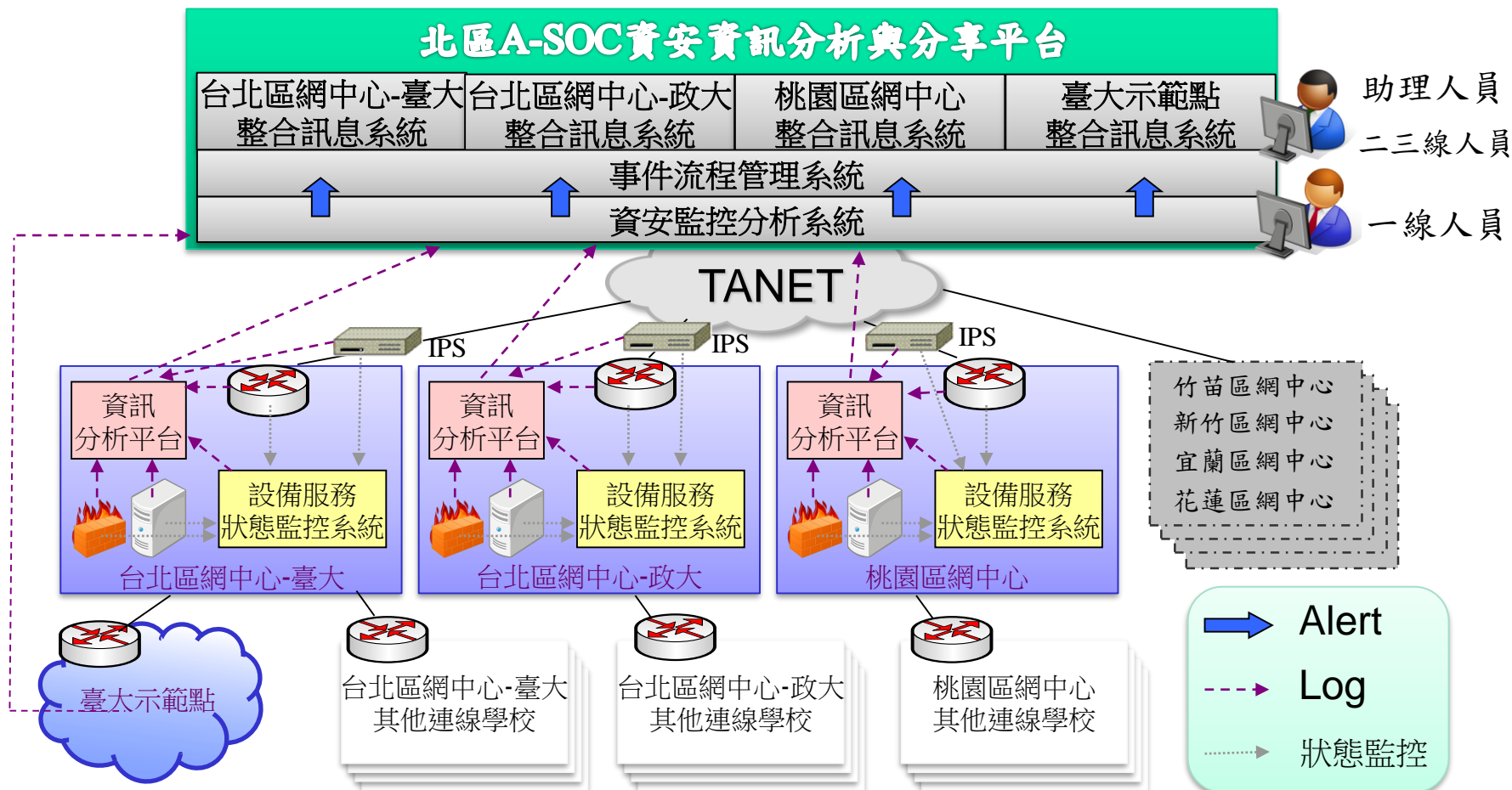
Critical Active



建立北區A-SOC資訊安全警訊通報機制

- 依據「國家資通安全會報通報與應變作業流程」進行資安事件處理，進而建立北區A-SOC通報與應變作業流程
 - 一般資安事件(1、2級)：應於1小時內進行通報，並於72小時內復原或完成損害管制。
 - 重大資安事件(3、4級)：應於1小時內進行通報，並於36小時內復原或完成損害管制。
 - 緊急資安事件：包含惡意程式攻擊、非經授權的存取、資訊作業服務遭惡意中斷、網站或資料遭竄改或刪除時及重要資料遭竊取等應緊急處理事件。
- 主動將最新資安訊息透過A-ISAC通告，同時迅速利用電話、簡訊、電子郵或傳真等方式，提供各監控點預警與通報之服務。

A-SOC資安資訊分析與分享平台架構



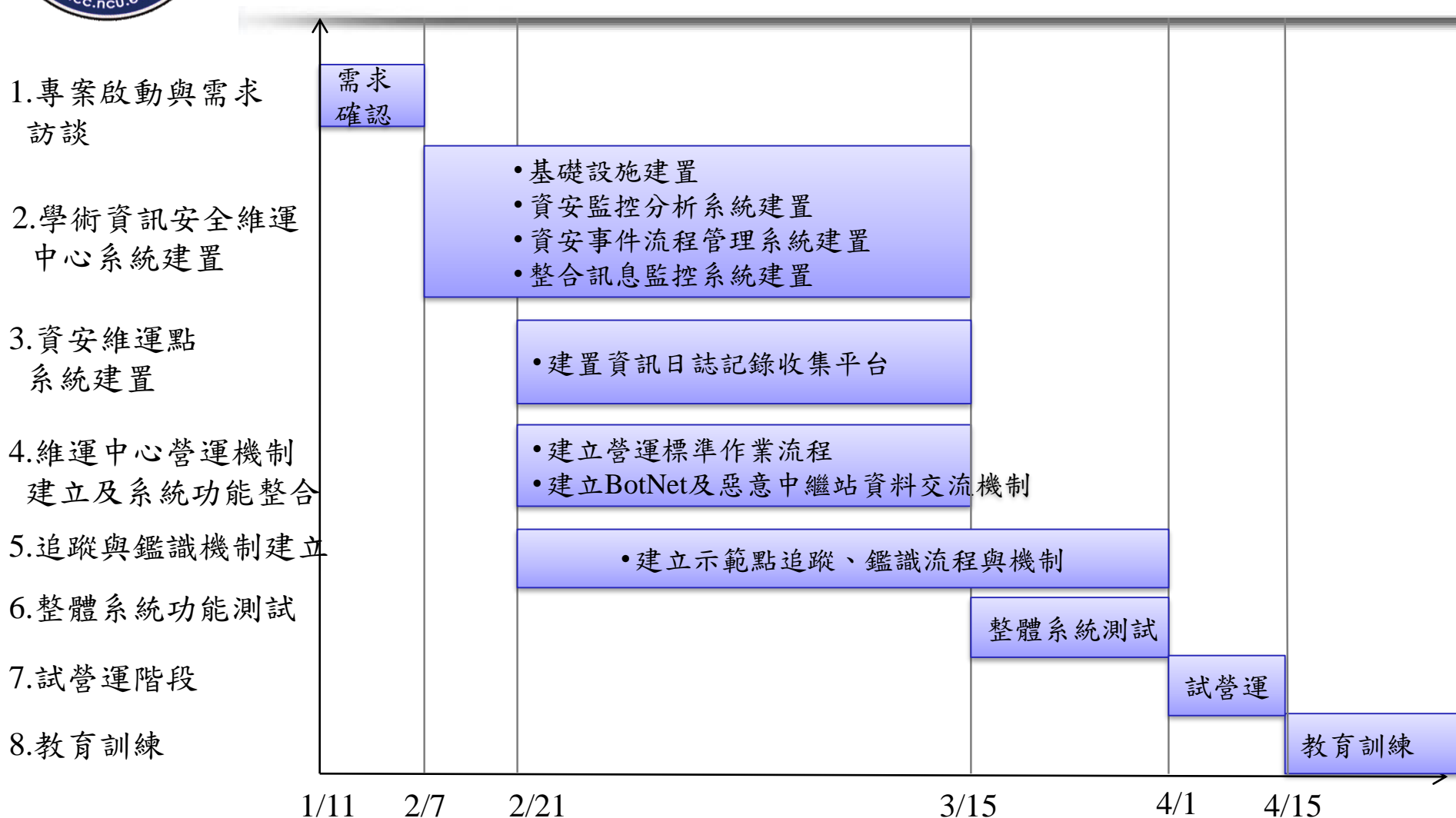


建置北區A-SOC資訊安全監控環境

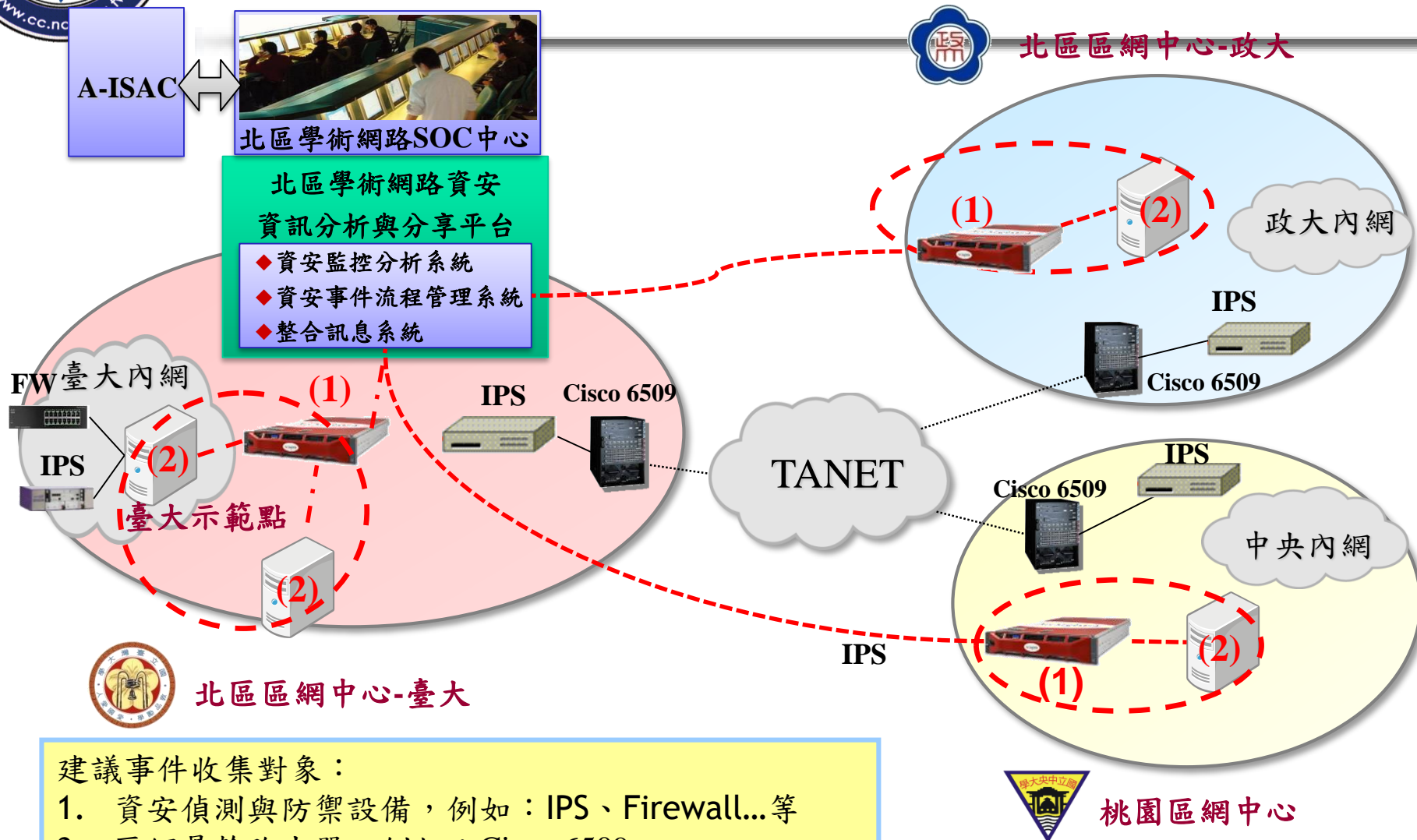
- 建置北區A-SOC資安監控中心軟硬體設施，包含資安監控分析平台、資安事件流程管理平台以及資安資訊分析與分享平台。
- 中華電信99/12得標建置



專案建置時程與重要里程碑



資安維運點建置



建議事件收集對象：

1. 資安偵測與防禦設備，例如：IPS、Firewall...等
2. 區網骨幹路由器，例如：Cisco 6509



進駐設備介紹

- 資訊日誌收集器
 - ArcSight Connector x1 (HP DL360 G7 / Windows 2008)
 - 1U, 110V雙電源, 1G電介面乙太網路
 - 提供Syslog、SNMP、ODBC、Log File等方式收集事件紀錄並給予標準化



進駐設備介紹

- 資訊日誌記錄收集平台
 - ArcSight Logger L3200 x1
 - 2U, 110V雙電源, 1G電介面乙太網路
 - 集中收集儲存所有監控設備的日誌
 - 提供1TB 儲存空間保存6個月以上原始事件紀錄



Router

Switch

ISA

Firewall

IPS

AnitVirus

Security
Gateway

RSA

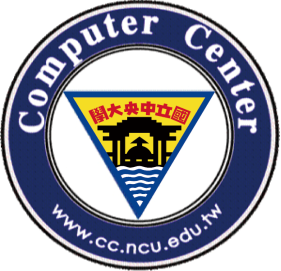
Databases

Snort



安裝時程

- ☐ 安裝時程：2/25
- ☐ 資訊安全M8000防護日誌(syslog)導入 日誌收集器 (Smart connector)：3/2



資通安全事件

□ 桃園區網2011-01-01~2011-04-19 共有51筆

- 國立中央大學 :22
- 中原大學 :5
- 萬能科技大學 :5
- 國立體育大學 :4
- 新興高級中學 :3
- 元智大學 :2
- 清雲科技大學 :2
- 中央警察大學 :1
- 青輔會青年職訓中心 :1
- 國立中壢高中:1
- 國立桃園農工 :1
- 銘傳大學 :1
- 開南大學 :1
- 成功高級工商 :1
- 國立楊梅高中:1



資通安全事件影響等級

□ 資通安全事件影響等級：

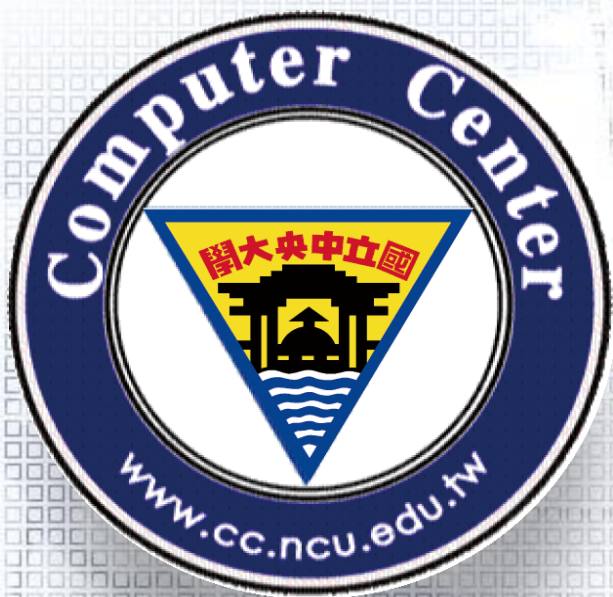
➤ 等級1:51

- (1) 機密性衝擊 -1級-非核心業務資料遭洩漏
- (2) 完整性衝擊 -1級-非核心業務系統或資料遭竄改
- (3) 可用性衝擊- 1級-非核心業務運作遭影響或短暫停頓



資通安全事件分類

INT-主機對外攻擊	14
其它-Spammer	12
DEF-惡意留言	6
DEF-惡意留言	4
DEF-釣魚網站	3
INT-主機被入侵	2
DEF-網頁置換	2
DEF-惡意網頁	2
INT-社交工程攻擊	2
INT-主機針對性攻擊	1
INT-其它	1
INT-C&C-IRC殭屍電腦控制程式	1
INT-主機針對性攻擊	1



建議事項



Computer Center, National Central University.



Thank You!