TANet

學術資安維運中心(A-SOC)
學網資安防護

臺灣大學計算機及資訊網路中心

李美雯

大綱

OUTLINE

北區ASOC簡介

入侵偵測防護

TANET DDoS 防護

漏洞通報與案例分享

資安能量整合

總結

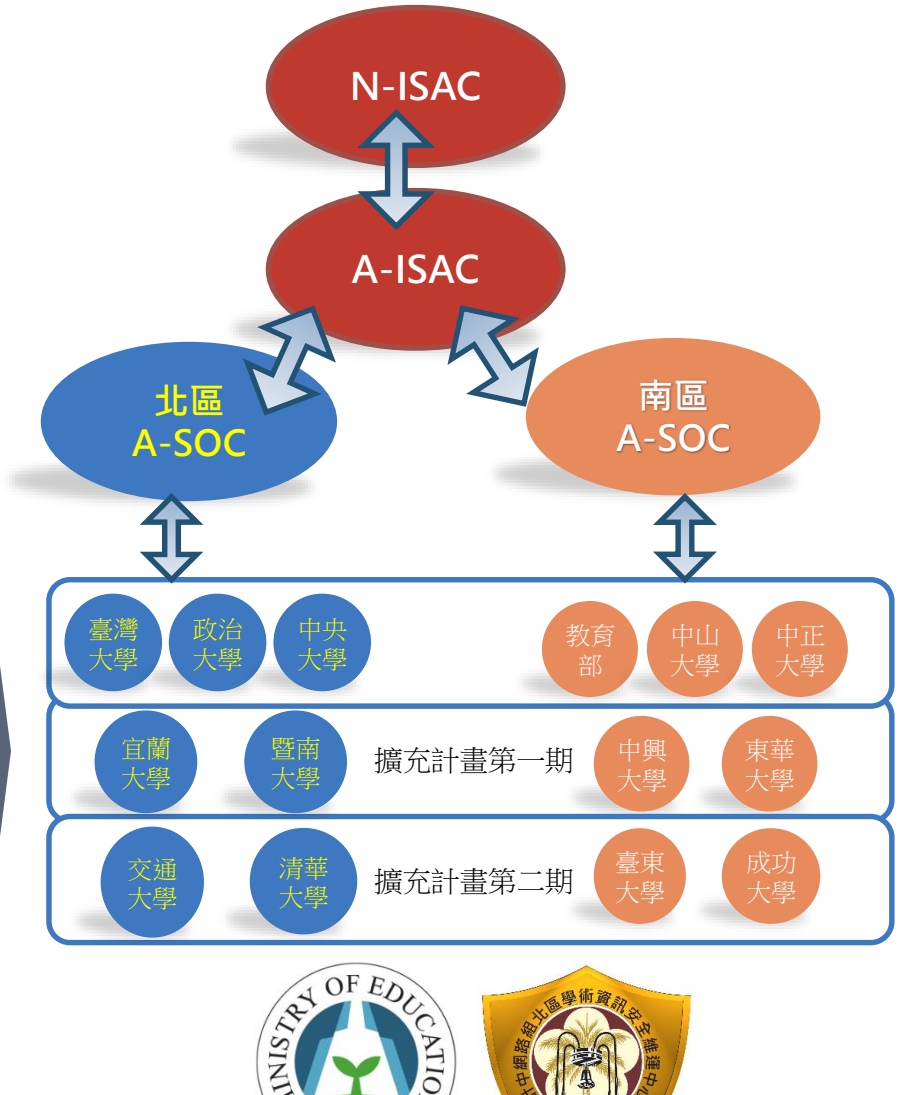
01

北區ASOC簡介

ASOC營運計畫

北區學術資訊安全維運中心（A-SOC）

- 本國**資安資訊分享與分析機制**由行政院**資通安全會報**統籌。教育部配合資安會報建置資安資訊分享與分析中心(A-ISAC)
- 教育部委託本校計資中心成立7×24營運之北區**學術資訊安全維運中心(A-SOC)**，建立**教育體系之資安防護及分析**機制，與**A-ISAC交換資安資訊**



計畫簡介

任務

偵測TANet骨幹網路入侵與攻擊

標準

「教育機構資安通報應變手冊」

- 1、2級事件
  72小時內處理完成並結案
- 3、4級事件
  36小時內處理完成並結案

範圍

七大區網中心(2896所學校)

- 臺北區網中心-1
- 臺北區網中心-2
- 桃園區網中心
- 宜蘭區網中心
- 新竹區網中心
- 竹苗區網中心
- 南投區網中心

成果

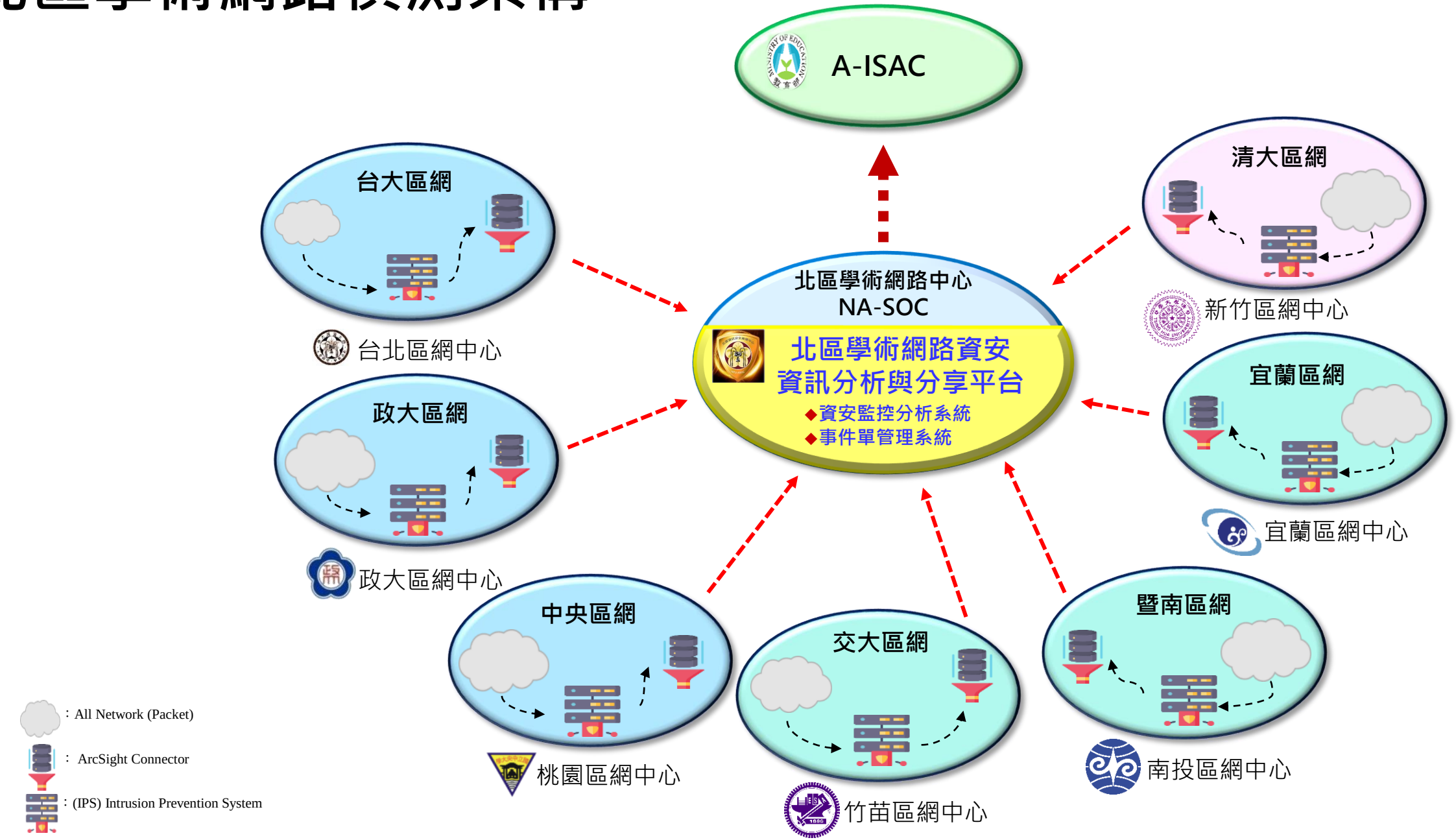
近三年開立情資單

- 109年度 件
- 110年度 件
- 111年度 件

02

入侵偵測防護

北區學術網路偵測架構


A-ISAC
台大區網
台北區網中心
清大區網
新竹區網中心
北區學術網路中心
NA-SOC
北區學術網路資安
資訊分析與分享平台
◆資安監控分析系統
◆事件單管理系統
政大區網
政大區網中心
宜蘭區網
宜蘭區網中心
中央區網
桃園區網中心
交大區網
竹苗區網中心
暨南區網
南投區網中心
：All Network (Packet)
： ArcSight Connector
：(IPS) Intrusion Prevention System

資安情資偵測與通報架構

通報學校

TACERT

A-ISAC

通報單管理系統

資安監控分析系統

正規化 資安情資

系統管理員

攻擊當下：阻擋攻擊
攻擊結束：情資處理

發生異常連線

連線到惡意中繼站報到

惡意程式發動攻擊

礦池IP連線

Drop

入侵偵測防禦系統
(Inline Drop)

正常連線

情資偵測與分析

01 TALOS

使用Cisco TALOS 情資，包含：IP、domain、URL、挖礦、釣魚、惡意bot等黑名單，每天即時更新。

02 SNORT

使用商業版Snort rule，目前共有五萬餘條規則，並即時更新動態調整規則，常態開啟之規則約有1萬餘條。

03 ArcSight & ELK

使用 ArcSight 情資整合平台，撰寫事件關聯規則，以及自動化流程；使用ELK視覺化資料庫，進行事件分析，以及大數據應用。

七大區網中心

使用 Sourcefire IPS，包含：台北、政大、桃園、竹苗、新竹、宜蘭、南投，占全台年度開單事件量 59% 以上。

Per day

100K
Snort rules intrusion events

17000K
Security intelligence events

03

TANET DDoS 防護

TANet DDoS 防禦

60Gbps
最大可清洗 60Gbps 攻擊加正常流量。

OOP (Out Of Path)

發現攻擊後，將流量導入清洗，平時不影響正常流量

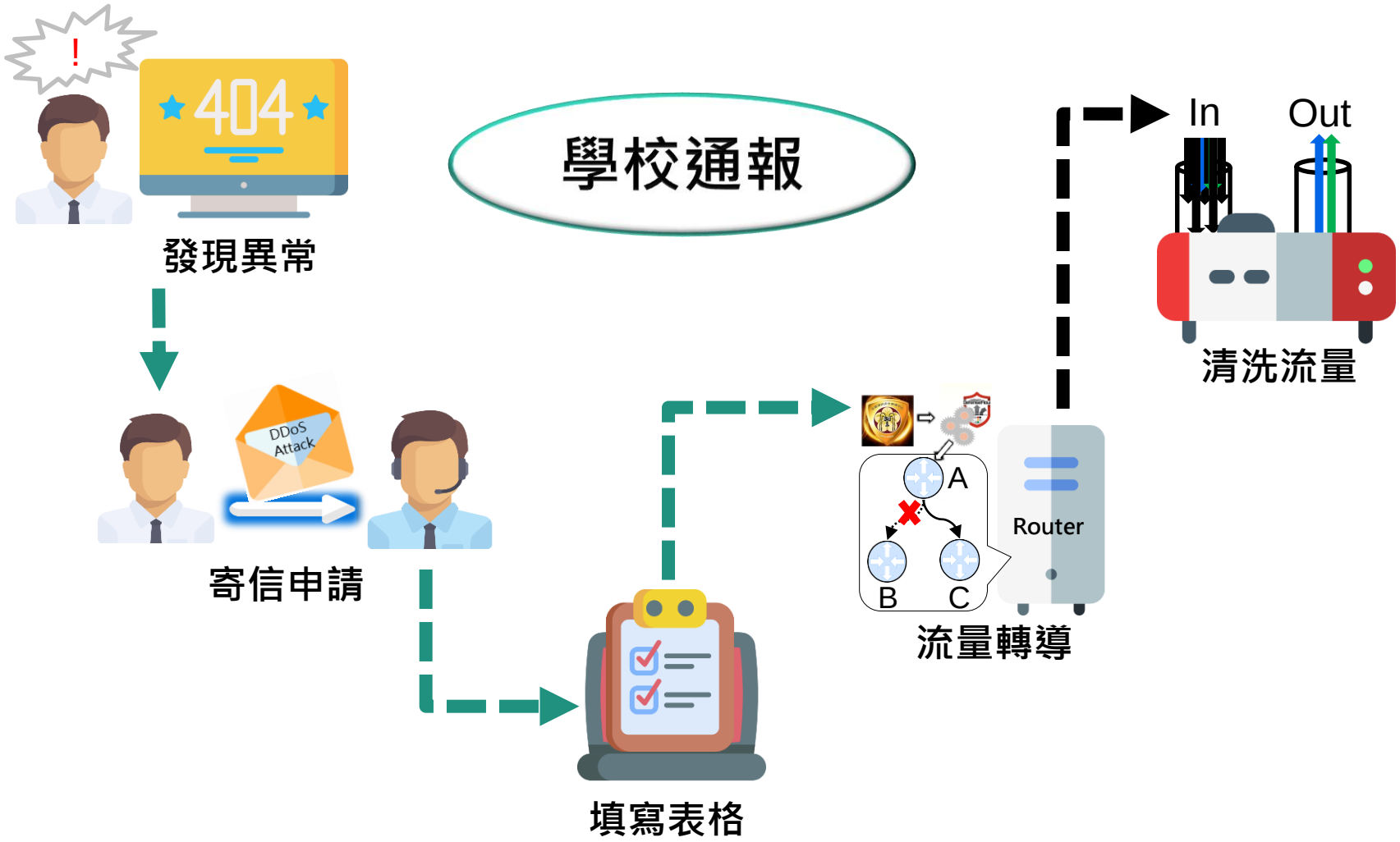
- 外對內
- 內對外
- 內對內 (搭配南北聯防)

針對TANet內外部DDoS威脅予以抑制

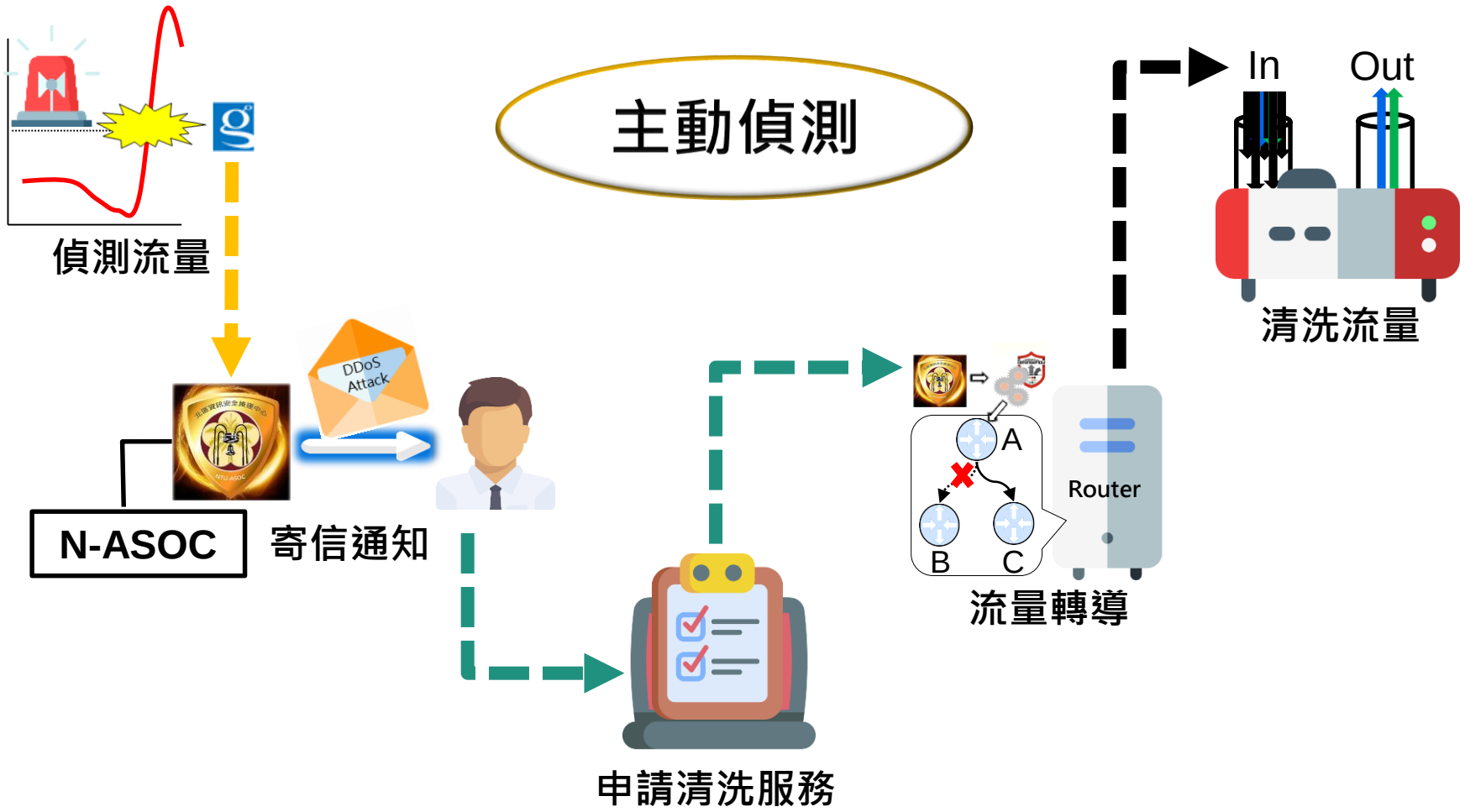
- A-SOC偵測通報
- 單位主動發現與通報
- 教育體系以外機關通報

遵循教育部「教育體系分散式阻斷服務防禦與應變作業規範」

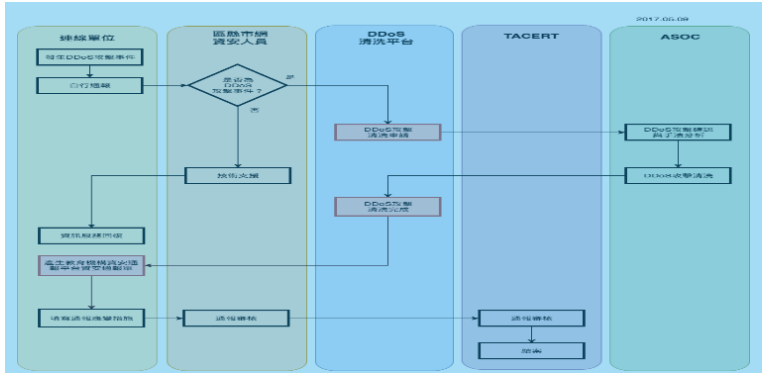
DDoS攻擊偵測與通報架構



DDoS攻擊偵測與通報架構

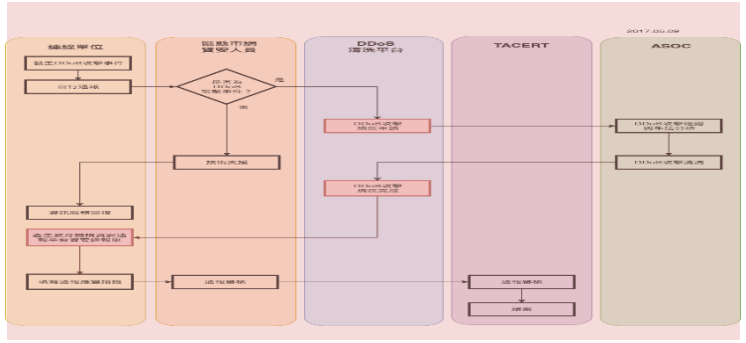


TANet DDoS攻擊防禦作業規定



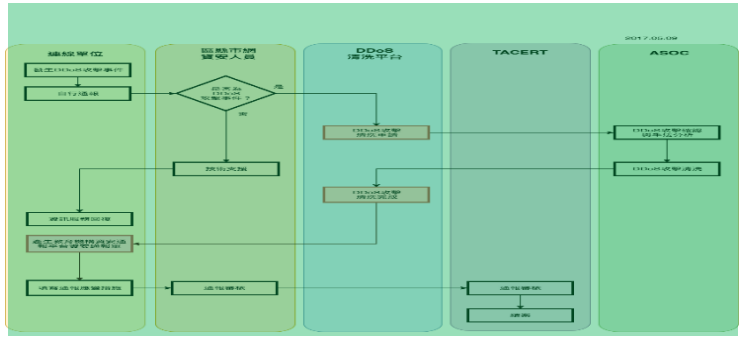
A-SOC主動偵測之通報與防禦

- 北區ASOC骨幹偵測DDoS攻擊後，與下轄單位確認後，執行攻擊流量清洗



單位自行通報之通報與防禦

- 單位自行發現DDoS攻擊， 通報區縣市網，確認後至**TACert**「資安通報系統」申請清洗作業



教育體系單位攻擊其他單位

- 外部單位透過TACERT，通知北區ASOC DDoS攻擊事件，並偕同區縣市網進行清洗作業

04

漏洞通報與案例分享

FTP 匿名登入-機敏資料曝光

建議措施

- 使用 FTP 服務時，**應關閉FTP匿名**、**預設帳號密碼**登入
- 定期更新設備、並資料備份，減少資料遺失的風險
- 非必要，**請勿將設備暴露於Internet中**
- 若需公開於網路中 ，請取消預設帳號密碼，並使用高強度帳密，**或限制設備存取 IP**

數位攝影機-空間隱私暴露

建議措施

- 修改**預設帳號密碼**
- 非必要，**請勿將設備暴露於Internet中**
- 若需公開於網路中 ，請**限制設備存取 IP**

總結

OWASP IOT Top 10 2018

OWASP

Internet of Things Top 10

1. 弱密碼 (Weak Guessable or Hardcoded Passwords)
2. 不安全的網路服務 (Insecure Network Services)
3. 不安全的生態界面 (Insecure Ecosystem Interfaces)
4. 不安全的更新機制 (Lack of Secure Update Mechanism)
5. 使用不安全的元件 (Use of Insecure Outdated Components)
6. 隱私防護不足 (Insufficient Privacy Protection)
7. 不安全的資料轉移和儲存 (Insecure Data Transfer and Storage)
8. 缺乏裝置設定 (Lack of Device Settings)
9. 不安全的預設 (Insecure Default Settings)
10. 缺少物理加固措施 (Lack of Physical Hardening)

QNAP NAS重大漏洞 (CVE-2022-27593)

QNAP NAS重大漏洞(CVE-2022-27593)

QNAP NAS於 9/3釋出 Photo Station漏洞警訊，編號 CVE-2022-27593，CVSS風險值達最高分10分
目前已知 DeadBolt勒索軟體針對此漏洞進行攻擊，已有災情傳出，
北區 ASOC發現貴區網轄下 IP(附件一)有 QNAP產品暴露於 Internet中，
請老師盡速通報，並參考以下措施，避免遭受駭客攻擊。

受影響版本：
QTS 5.0.1：Photo Station 6.1.2 及更高版本
QTS 5.0.0/4.5.x：Photo Station 6.0.22 及更高版本
QTS 4.3.6：Photo Station 5.7.18 及更高版本
QTS 4.3.3：Photo Station 5.4.15 及更高版本
QTS 4.2.6：Photo Station 5.2.14 及更高版本

建議使用者盡速更新韌體，並進行以下措施：
1. 避免將 QNAP NAS暴露在公開網路上，將設備放置於內部網路並使用VPN從外部連線存取。
2. 更新 QTS所有應用程式至最新版本。
3. 定期備份 NAS中的資料。
4. 啟用系統連線記錄，管理人員留意登入警訊。
5. 透過啟用 NAS「IP存取保護」，可以自動封鎖在特定時間內多次登入失敗的 IP。

居易 (DrayTek) 路由器重大漏洞 (CVE-2022-32548)

居易 (DrayTek) 路由器重大漏洞(CVE-2022-32548)

老師您好，

居易路由器近期出現 CVSS 風險評分達10分之漏洞，
web 管理頁面存在 RCE 漏洞，
可被攻擊者遠端執行程式碼，獲得系統控制權，
北區 ASOC 發現貴區網轄下 IP 疑似有居易科技之路由器暴露於網路上 (如附檔)

請區網老師協助通報轄下單位進行相關緩解措施：

1. 居易已釋出更新檔，請使用者盡速更新：
   https://www.draytek.com/support/latest-firmwares/
2. 建議 web 頁面避免暴露在 Internet 上，或限制存取 IP。

05

資安能量整合

資安意識強化及資安技術交流

出處:北區ASOC整理

06

結論

一. 持續**資安事件**分析、檢測、通報

二.持續調教DDoS設備**偵測準確率**

三.持續更新和蒐集各方**情資**，阻擋連線以降低資安風險

四. 協助**IoT設備**檢測與漏洞分析

五.持續與各資安團隊共同強化資安**應變處理能量**

六. 協助開設**資安相關課程**，針對學術網路環境中存在之資安風險與個資外洩之疑慮，宣導正確的電腦使用習慣。


MINISTRY OF EDUCATION
教育部


台中網路組北區學術資訊安全維運中心
NTU-ASOC


Q&A