學術網路Snort推廣與應用

主講人–曲成權、李柏毅

2012.07.12

大綱

- 入侵偵測系統簡介
- Snort 介紹
- 已建制個案分享
- 後續研究與發展
- 建置技術移轉

A-SOC計畫

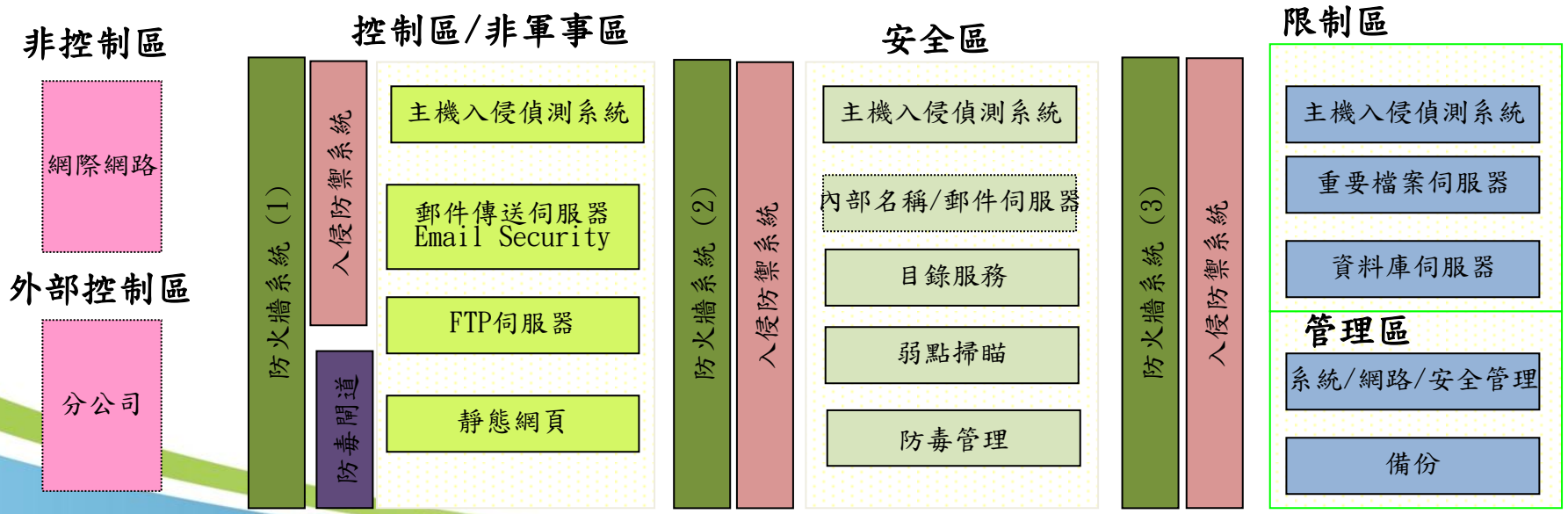
- 國家高速網路與計算中心受教育部電算中心委託辦理『**教育部98年度教育學術資訊安全監控中心(A-SOC)暨殭屍電腦(Botnet)防禦機制建制計畫**』，負責偵測學術網路的網路攻擊並發出警訊。
- 目前有南區A-SOC(國網中心)與北區A-SOC(臺大計中)。

網路安全面臨的問題

- 病毒蠕蟲攻擊
- 網路癱瘓
- 垃圾郵件
- 機密外洩
- 非法入侵
- 即時通訊
- 點對點傳輸
- ....

常見資安設備

- 防火牆－僅讓允許的流量通過經過
- 入侵偵測/防禦系統－監控網路上攻擊行為
- 主機入侵偵測防禦－監控重要系統資源
- 稽核事件－啟動稽核記錄(Windows Event Log, UNIX Syslog /Audit Trail)
- 弱點掃瞄－確實瞭解系統漏洞
- 防毒牆 / 防毒管理－防護病毒感染
- 郵件安全－提供過濾、防毒、內容管理…等功能
- 安全管理－SIEM 平台



防火牆無法阻擋的網路攻擊

- 通訊埠掃瞄攻擊(Port Scans)
- 系統及應用程式弱點攻擊(System and Application Vulnerabilities Attack)
- 緩衝區溢位攻擊(Buffer Overflows Attack)
- 木馬程式攻擊(Trojan Horses Attack)
- 蠕蟲攻擊(Worms Attack)
- ….

IDS 簡介

- **入侵偵測（Intrusion Detection System, IDS)：**
  是對電腦網路和電腦系統的通訊資訊進行收集，分析其中是否有攻擊或違反安全策略的事件。
  - 監控網路上用戶和系統的所有活動
  - 將封包拆開分析再重新組合
  - 依靠特徵碼或規則(Signature,Rule) 進行防護
- **NIDS 及 HIDS**
  - 網路型入侵偵測系統Network-based IDS,簡稱NIDS
  - 主機型入侵偵測系統Host-based IDS,簡稱HIDS

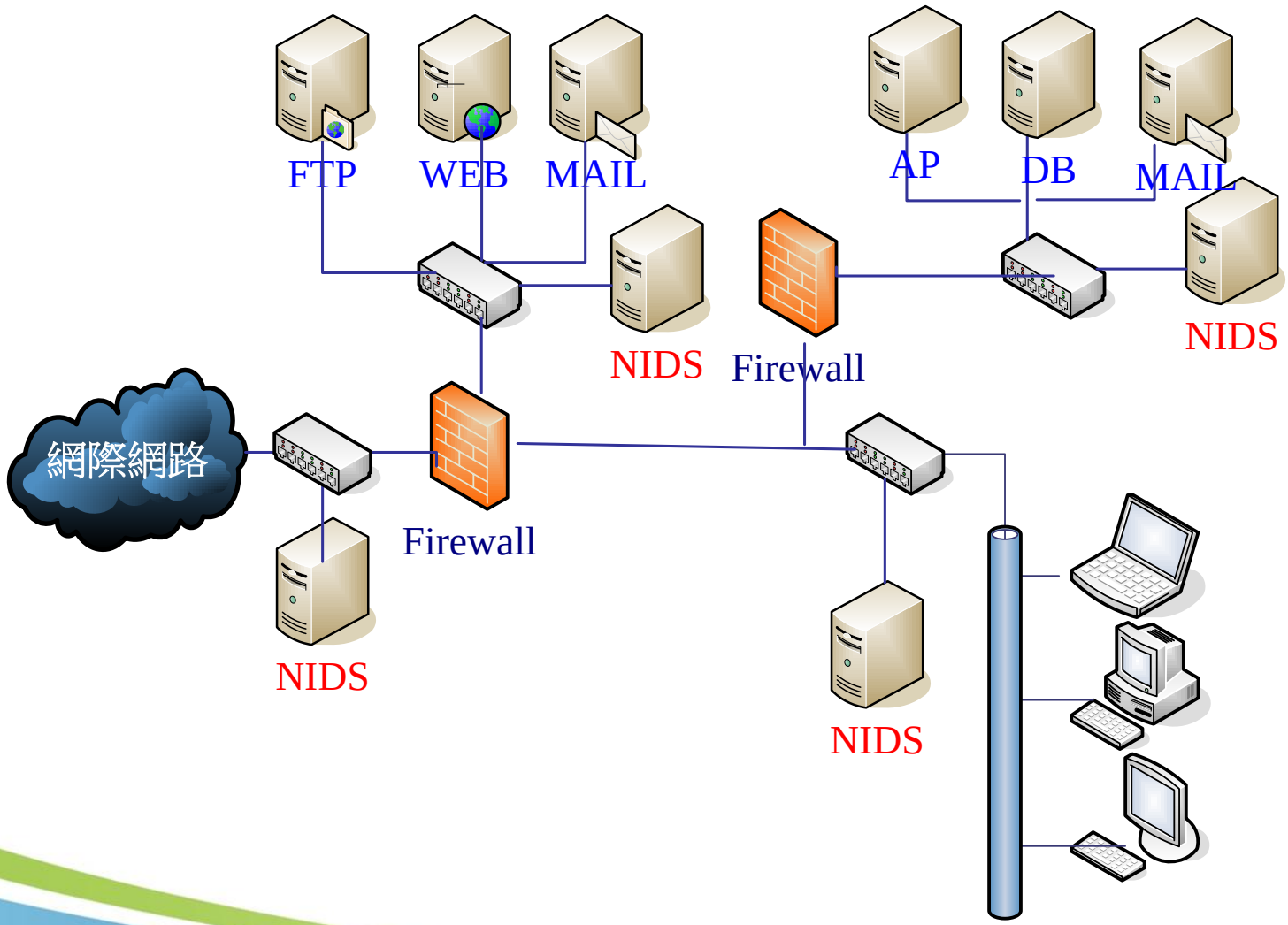
IDS 提供之功能

- **監控網路(NIDS)和系統(HIDS)**
  - 發現入侵企圖或異常現象
  - 主動告警，通知系統管理者現在網路狀況
  - 將攻擊或異常紀錄下來進行分析
- **防火牆功能不足**
  - 無法阻擋合法網路連結
  - 對於弱點攻擊的保護較難
  - 不是所有的威脅均來自防火牆外部
- **現在網路入侵很容易**
  - 各種駭客工具垂手可得
  - 入侵書籍及網站隨處可見

標準 IDS 運作方式

- 安裝於需要保護的網段中
- 混亂模式(Promiscuous)監聽
  - a configuration of a network card that makes the card pass all traffic it receives to the kernel rather than just frames addressed to it (http://en.wikipedia.org/wiki/Promiscuous_mode)
- 分析經過這網段的所有封包
- 不影響網段中主機的運作

IDS 佈署示意圖


FTP
WEB
MAIL
AP
DB
MAIL
NIDS
Firewall
NIDS
網際網路
Firewall
NIDS
NIDS

IDS 監控模式限制

- 缺乏主動防禦能力：IDS只有告警的能力，無法中斷入侵行為。
- 誤報率偏高：利用特徵碼以判斷是否為入侵行為，但有些正常封包的特徵和入侵行為的特徵十分類似。
- 對未知攻擊手法無效：目前的IDS系統還無法有效的識別出未知的入侵，也就是造成安全假象。
- 加密封包無法辨識：因IDS是根據網路封包進行分析的，如果封包經過加密，就無法辨識其內容，也就無法進行分析

→ **Intrusion Prevention System，IPS**，可主動偵測入侵行為並主動防禦

Snort簡介

- Snort是一套開放的(Open Source)、跨平台（Uinx, Windows…)的NIDS，可用來偵測網路上的異常封包，1998年由Marty Roesch開發，全球下載超過四百萬次。
- 檢查所有經過的封包，並利用特徵比對的方式判斷是否有可能的入侵行為
- 規則是開放的方式來發展的，可以自行加入偵測規則，以加強入侵行為的偵測
- SNORT官方網站：http://www.snort.org/

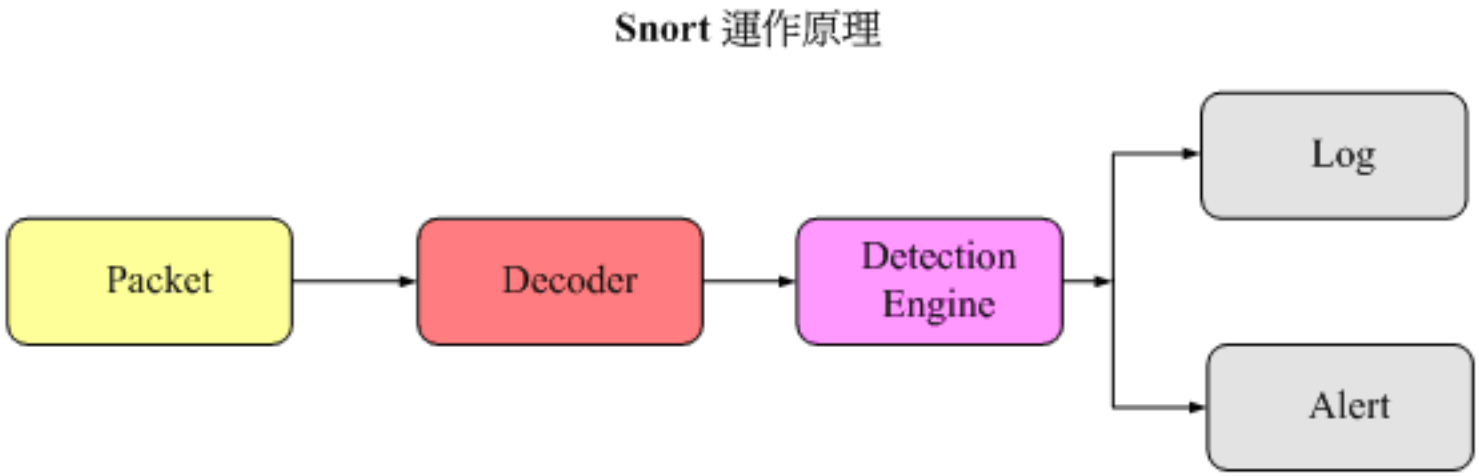
Snort運作模式

Snort可以三個模式進行運作，本案安裝以入侵偵測模式：

- 偵測模式：此模式下，Snort將在現有的網域內擷取封包，並顯示在螢幕上。
  - snort -dev
- 封包紀錄模式：此模式下，Snort將已擷取的封包存入儲存媒體中（如硬碟）。
  - snort –dev –l ./log
- 入侵偵測模式：此模式下，Snort可對擷取到的封包做分析的動作，並根據一定的政策來判斷是否有網路攻擊行為的出現。

Snort運作原理

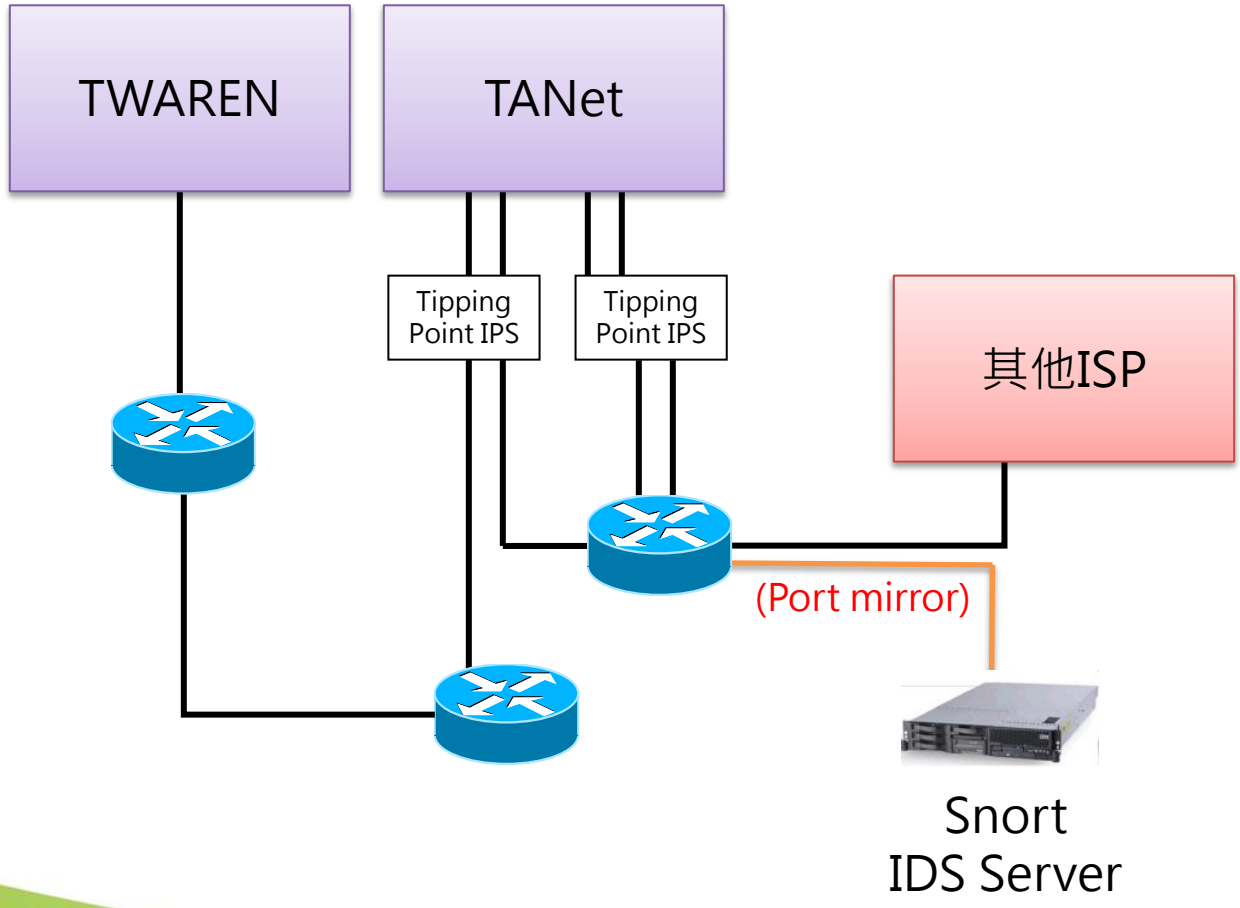
- Snort先收集網路封包後、解碼就進行分析，並根據分析結果進行紀錄（Log）及警示（Alert）



Snort標準偵測規則

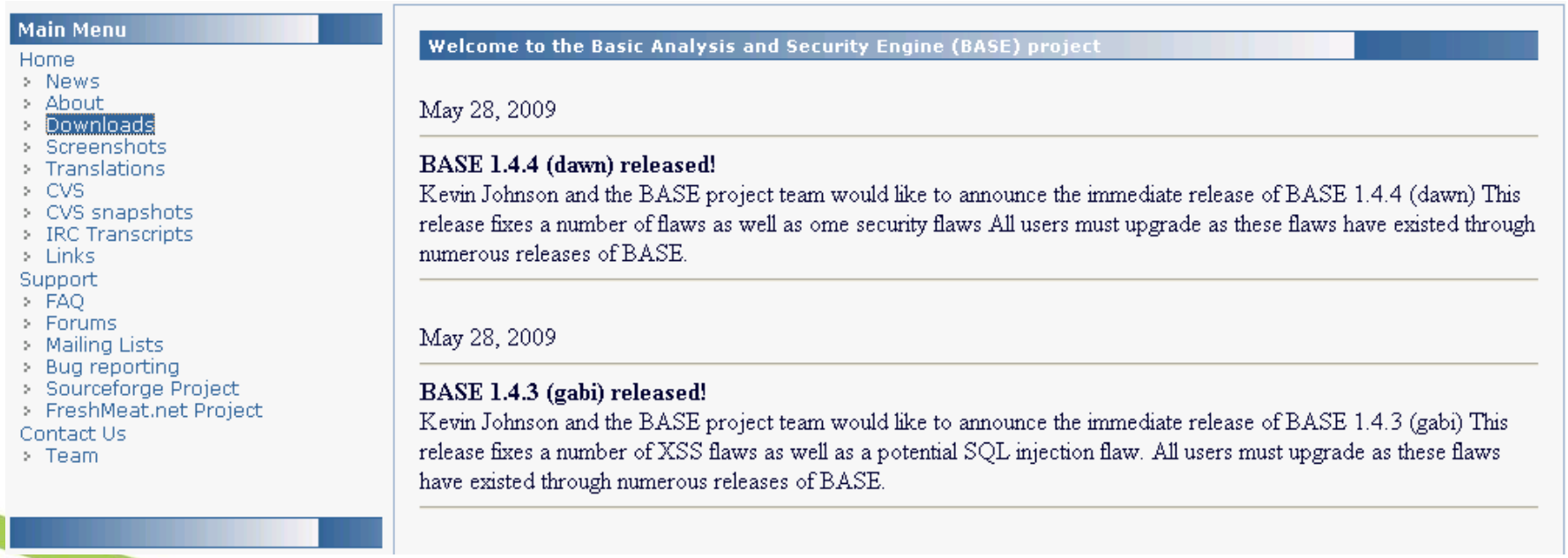
通訊協定偵測	攻擊	其他(病毒，內容過濾)
chat.rules	attack-responses.rules	bad-traffic.rules
dns.rules	backdoor.rules	experimental.rules
finger.rules	ddos.rules	info.rules
icmp.rules	dos.rules	local.rules
icmp-info.rules	exploit.rules	misc.rules
imap.rules	scan.rules	other-ids.rules
multimedia.rules	shellcode.rules	policy.rules
mysql.rules	web-*.rules	porn.rules
netbios.rules		virus.rules
nntp.rules		
oracle.rules		
p2p.rules		
pop2.rules		
pop3.rules		
rpc.rules		
rservices.rules		
smtp.rules		
sql.rules		
telnet.rules		
tftp.rules		
web-*.rules		
x11.rules		

中正大學Snort系統部署架構圖



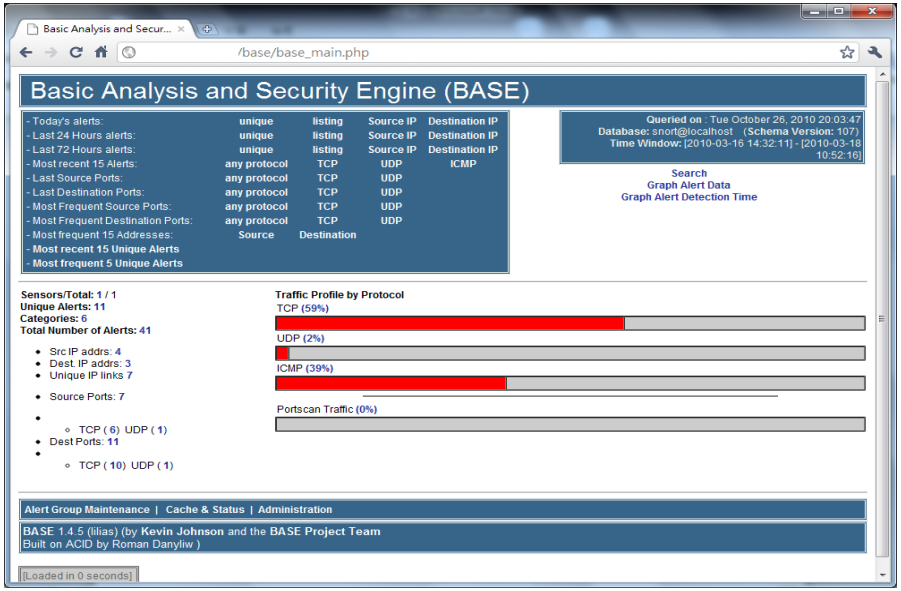
Snort Log分析

- Basic Analysis and Security Engine （BASE）
  - 官方網站:http://base.secureideas.net/
  - It is based on the code from the Analysis Console for Intrusion Databases (ACID) project



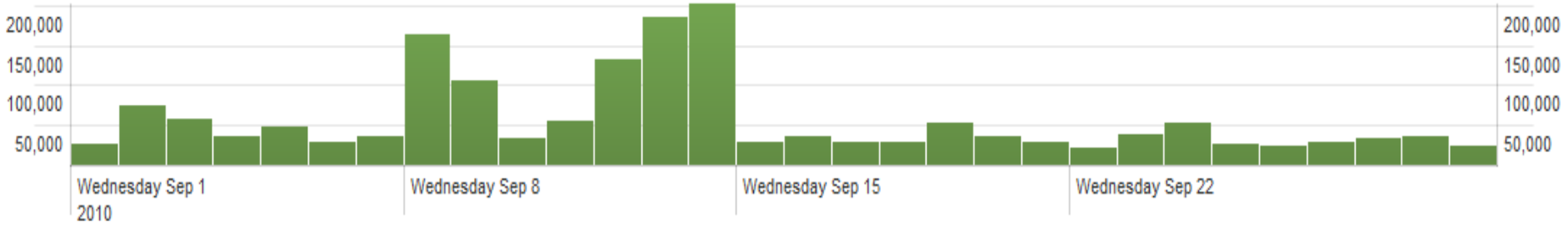
Snort Log分析

- BASE的前身為ACID計畫(Analysis Console for Intrusion Databases)
- 資料來源：Snort 存入MySQL 資料庫內容
- 透過瀏覽器來顯示分類、統計與繪圖
- 圖形化的使用者界面



Snort Log分析

- Splunk

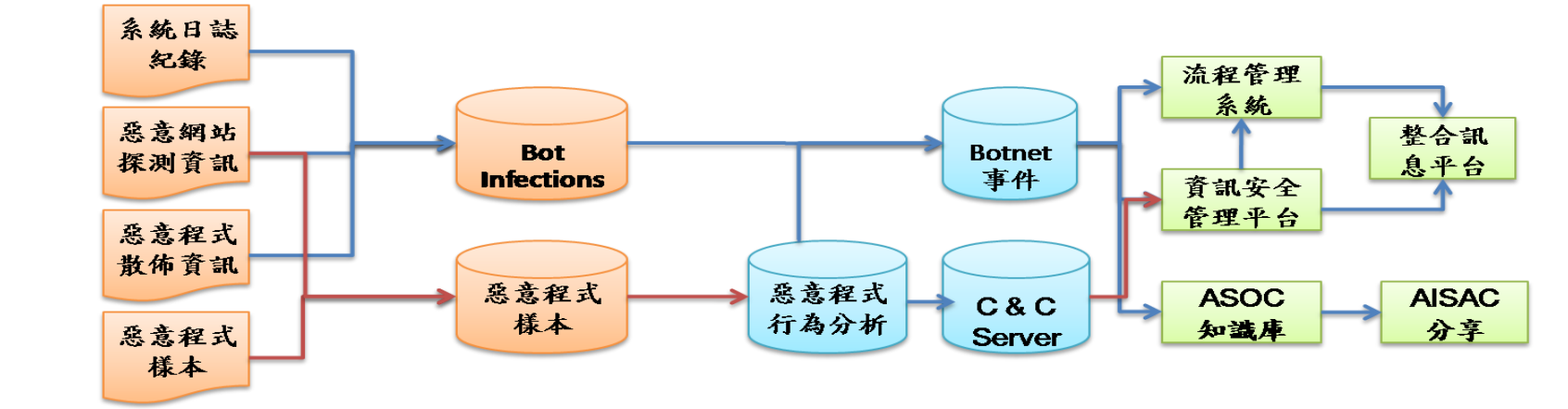



```
Oct 26 14:51:11 IBM-Snort snort[29527]: [1:5000002:0] TR.Crypt.XPACK.Gen.20100119 DNS1 {UDP} 163.27.140.4:49876 -> 168.95.1.1:53
Oct 26 14:51:11 IBM-Snort snort[29527]: [1:5000036:0] TR.Crypt.ZPACK.Gen.7.20100204 {UDP} 140.130.159.57:32768 -> 168.95.192.1:53
Oct 26 14:51:12 IBM-Snort snort[29527]: [1:5000002:0] TR.Crypt.XPACK.Gen.20100119 DNS1 {UDP} 61.220.4.90:35298 -> 163.27.140.1:53
Oct 26 14:51:13 IBM-Snort snort[29527]: [1:5000002:0] TR.Crypt.XPACK.Gen.20100119 DNS1 {UDP} 163.27.76.1:1028 -> 168.95.1.1:53
Oct 26 14:51:13 IBM-Snort snort[29527]: [1:5000002:0] TR.Crypt.XPACK.Gen.20100119 DNS1 {UDP} 140.130.81.11:47050 -> 168.95.1.1:53
Oct 26 14:51:14 IBM-Snort snort[29527]: [1:2003055:5] ET MALWARE Suspicious 220 Banner on Local Port [Classification: Detection of a non-standard protocol or
event] [Priority: 2]: {TCP} 140.123.244.186:10050 -> 211.75.103.13:50425
Oct 26 14:51:16 IBM-Snort snort[29527]: [1:5000002:0] TR.Crypt.XPACK.Gen.20100119 DNS1 {UDP} 163.27.76.1:1028 -> 168.95.1.1:53
Oct 26 14:51:16 IBM-Snort snort[29527]: [1:5000002:0] TR.Crypt.XPACK.Gen.20100119 DNS1 {UDP} 163.27.140.4:49982 -> 168.95.1.1:53
Oct 26 14:51:16 IBM-Snort snort[29527]: [1:5000002:0] TR.Crypt.XPACK.Gen.20100119 DNS1 {UDP} 61.220.4.44:8747 -> 163.27.140.1:53
Oct 26 14:51:16 IBM-Snort snort[29527]: [1:5000002:0] TR.Crypt.XPACK.Gen.20100119 DNS1 {UDP} 163.27.140.4:49990 -> 168.95.1.1:53
Oct 26 14:51:16 IBM-Snort snort[29527]: [1:5000002:0] TR.Crypt.XPACK.Gen.20100119 DNS1 {UDP} 61.220.4.29:4822 -> 163.27.140.1:53
Oct 26 14:51:16 IBM-Snort snort[29527]: [1:5000003:0] TR.Crypt.XPACK.Gen.20100119 DNS2 {UDP} 163.27.152.6:57372 -> 168.95.1.1:53
```

中正大學目前Snort規則來源

- Malware Threat Center
  - http://mtc.sri.com/
  - 規則下載： http://www.emergingthreats.net/rules/
- Emerging Threats
  - http://www.emergingthreats.net/
  - 規則下載： http://mtc.sri.com/live_data/signatures/
- 系統安全與惡意程式偵測紀錄研發建置計畫
  - http://www.botnet.tw/
  - 規則下載：
    http://www.botnet.tw/content/botnet_rule.php

Botnet偵測與應變



Botnet Honeypot
- Honeywall
- Malware Honeypot
- Client Honeypot
- 高互動式Win32 HP
- 高互動式Linux HP

監控點資訊分析系統
- Bot Infections分析
- Anti-Virus Detection
- 惡意網站判別
- 系統日誌分析

資訊分析平台
- Bot Infections 關聯分析
- FSA & Botnet聚合
- Botnet 事件分析
- C&C Server分析
- 快速變動惡意網域分析

惡意程式檢測系統
- 惡意程式行為分析
- Botnet 通訊連線分析
- 惡意程式反組譯

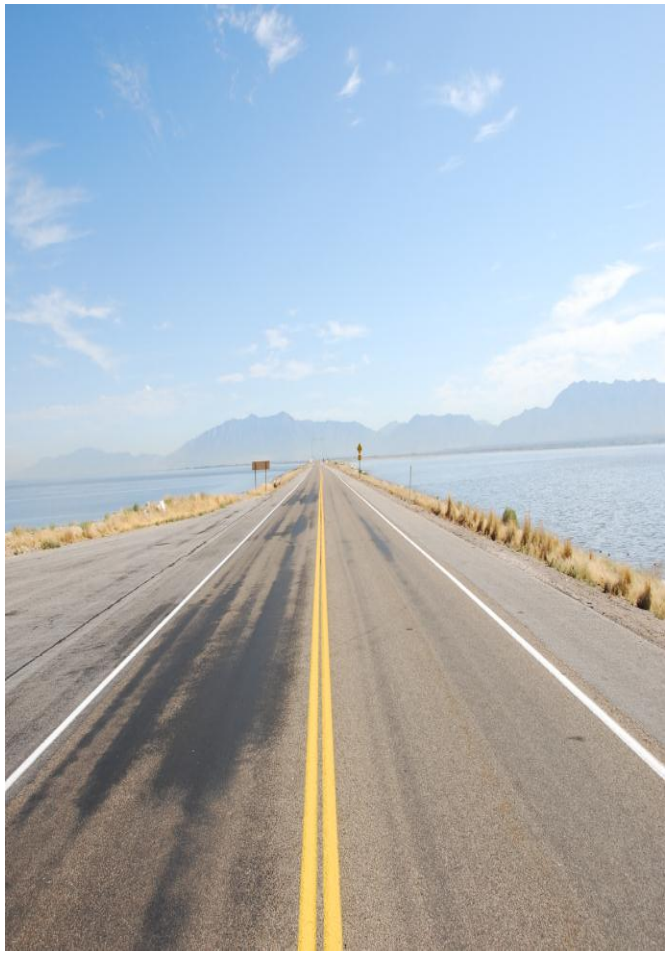
資訊分析平台
- 監控點事件統計
- 趨勢報表產生
- ASOC整合事件通報

A-ISAC分享
- ASOC知 識庫

橘色: 監控點工作流程與資料產出
藍色: SOC端工作流程與資料產出

後續研究與發展

- 學術網路事件回應與處理
- 資訊安全訊息分析
- 資訊安全技術交流
- 惡意程式分析
- Botnet偵測與清除



拍攝於：鹽湖城

建置技術移轉

- 移轉範圍
  - Snort套件安裝協助
    - Snort、BASE
  - Botnet規則提供
  - 協助資料分析
- 聯絡窗口
  - 台灣學術網路資訊安全維運中心
  - 0800-050940

Q & A

Thank You!!