

F A R E A S T O N E

遠傳

Mobile · Broadband · Media · International Service

新北市政府教育局  
資訊安全整合防護委外服務計畫

教育訓練簡報  
(資安服務)

杜建樺

2016.08.18

# 簡報大綱

- 一、SSO登入
- 二、案件處理
- 三、資產儀表板
- 四、資安新聞資訊
- 五、Q&A



# 一、SSO登入(1)

輸入網址：soc.ntpc.edu.tw

新北市教育局  
Education Bureau, New Taipei City

帳號：

密碼：

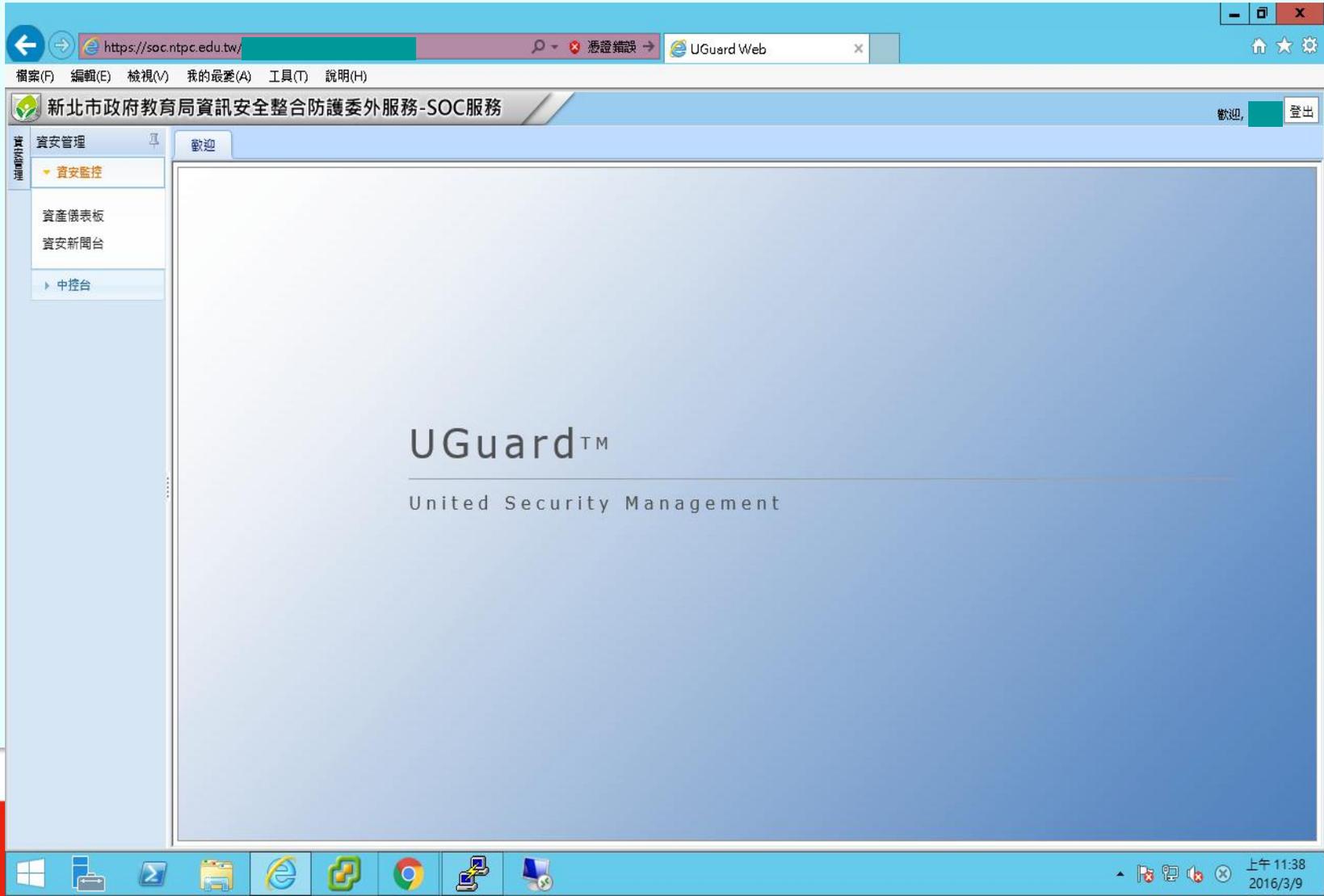
登入

單一認證入口  
*Single Sign-On*

# 一、SSO登入(2)

輸入網址：soc.ntpc.edu.tw



## 二、案件處理(1)

點選[中控台][訊息管理][待簽核表單]

The screenshot shows a web browser window with the URL <https://soc.ntpc.edu.tw/>. The page title is "新北市政府教育局資訊安全整合防護委外服務-SOC服務". The interface includes a navigation menu on the left, a main content area, and a taskbar at the bottom.

Navigation steps are indicated by red boxes and numbers:

1. Click on "中控台" (Dashboard) in the left navigation menu.
2. Click on "訊息管理" (Message Management) in the left navigation menu.
3. Click on "待簽核表單" (Pending Approval Forms) in the "訊息通知" (Message Notification) sub-menu.

The main content area displays a table with the following columns: "寄送時間" (Delivery Time), "機組描述" (Equipment Description), "表單單號" (Form Number), "主旨" (Subject), "寄件人" (Sender), and "說明" (Description). The table is currently empty, showing "沒有任何資料" (No data).

At the bottom of the page, the Windows taskbar shows the system tray with the date and time: 上午 11:38, 2016/3/9.

## 二、案件處理(2)

點選[表單單號]或[主旨]以開啟案件詳細資訊

新北市政府教育局資訊安全整合防護委外服務-SOC服務

歡迎, [Name] 登出

資訊管理 歡迎 訊息管理

案件追蹤與建立 資訊監控 黑白名單機制 中控制台 訊息管理 新增表單 機組管理

待審核表單 已審核表單 已結案表單 通知 原稿追蹤 自訂收件匣

表單批次審核 刪除 查詢 計時器設定 重新整理

寄送時間	機組描述	表單單號	主旨	寄件人	說明
2016/03/04 11:51:20	UGuard2	1143	第二級[阻斷服務攻擊案件]案件	Sy	[163.31.136.3]_B) 偵測到, 來源為[163.31.136.3]
2016/03/04 11:36:17	UGuard2	1145	第二級[後門/間諜程式行為]案件	Sy	[163.31.136.3]_A) 偵測到, 來源為[163.31.136.3]
2016/03/04 11:35:59	UGuard2	1145	第二級[後門/間諜程式行為]案件	Sy	[163.31.136.3]_A) 偵測到, 來源為[163.31.136.3]
2016/03/04 11:25:37	UGuard4	783	第二級[過量病毒無法移除]案件	Sy	[203.113.1.1] 偵測到, 來源為[0], 目的為[203.113.1.1]
2016/03/04 11:22:02	UGuard1	265	第二級[後門/間諜程式行為]案件	Sy	[163.31.136.3] RX-5600) 偵測到, 來源為[163.31.136.3]
2016/03/04 11:22:00	UGuard1	265	第二級[後門/間諜程式行為]案件	Sy	[163.31.136.3] RX-5600) 偵測到, 來源為[163.31.136.3]
2016/03/04 11:05:00	UGuard1	267	第二級[後門/間諜程式行為]案件	Sy	[163.31.136.3] RX-5600) 偵測到, 來源為[163.31.136.3]
2016/03/04 10:57:24	UGuard1	268	第二級[後門/間諜程式行為]案件	Sy	[163.31.136.3] RX-5600) 偵測到, 來源為[163.31.136.3]
2016/03/04 10:57:21	UGuard1	268	第二級[後門/間諜程式行為]案件	Sy	[163.31.136.3] RX-5600) 偵測到, 來源為[163.31.136.3]
2016/03/03 08:30:14	UGuard4	787	第二級[過量病毒無法移除]案件	Sy	[203.113.1.1] 偵測到, 來源為[0], 目的為[203.113.1.1]
2016/03/03 08:27:00	UGuard4	786	第二級[過量病毒無法移除]案件	Sy	[203.113.1.1] 偵測到, 來源為[0], 目的為[203.113.1.1]
2016/03/02 09:48:57	UGuard4	785	第二級[病毒擴散]案件	Sy	[203.113.1.1] 偵測到, 來源為[0], 目的為[203.113.1.1]
2016/03/02 08:45:54	UGuard4	784	第二級[過量病毒無法移除]案件	Sy	[203.113.1.1] 偵測到, 來源為[0], 目的為[203.113.1.1]
2016/03/01 22:36:24	UGuard1	266	第二級[後門/間諜程式行為]案件	Sy	[163.31.136.3] RX-5600) 偵測到, 來源為[163.31.136.3]
2016/03/01 11:51:59	UGuard2	1142	第二級[阻斷服務攻擊案件]案件	Sy	[163.31.136.3]_A) 偵測到, 來源為[10.2.1.1]
2016/03/01 11:49:44	UGuard2	1141	第二級[阻斷服務攻擊案件]案件	Sy	[163.31.136.3]_B) 偵測到, 來源為[163.31.136.3]
2016/03/01 11:40:44	UGuard2	1140	第二級[阻斷服務攻擊案件]案件	Sy	[163.31.136.3]_A) 偵測到, 來源為[10.2.1.1]
2016/03/01 11:16:28	UGuard2	1139	第二級[阻斷服務攻擊案件]案件	Sy	[163.31.136.3]_B) 偵測到, 來源為[10.2.1.1]
2016/03/01 11:08:14	UGuard2	1138	第二級[阻斷服務攻擊案件]案件	Sy	[163.31.136.3]_B) 偵測到, 來源為[163.31.136.3]
2016/03/01 11:08:13	UGuard2	1137	第二級[阻斷服務攻擊案件]案件	Sy	[163.31.136.3]_A) 偵測到, 來源為[10.2.1.1]

頁數: 2 of 151 Go 第 21 ~ 40 筆, 總筆數: 3004

## 二、案件處理(3)

案件資訊包含案件時間、來源ip、目的ip及事件內容

The screenshot displays a web browser window with the URL 'spl...' and the page title '檢視表單(單號: 1143)'. The interface includes a menu bar with options like '檔案(F)', '編輯(E)', '檢視(V)', '我的最愛(A)', '工具(T)', and '說明(H)'. Below the menu is a toolbar with buttons for '審核送單', '加會簽', '表單附掛檔案', '檢視流程', and '編輯'.

The main content area shows the following details:

- 表單類型:** MSS-IDS (資安威脅管理流程)
- 表單狀態:** 審核中
- 關卡抵達時間:** 2016-03-04 11:51:20
- 主旨:** 第二級[阻斷服務攻擊案件]案件
- 表單敘述:** [163.202.305.00]偵測到,來源為[163.202.305.00],目的為[...es]
- 關卡意義:** 通報學校資安窗口案件資訊並處理

Below the form fields is a table with columns for '新增', '刪除', and '重新整理'. The table contains one entry with columns for '檢視', '處置...', '主機名稱', '資產...', 'Ext2', and 'Ext1'. The entry shows 'NTP...' as the host name and '163.2...' as the asset.

The '案件說明' section contains the following text:

目的IP遭受多次阻斷服務之攻擊行為,阻斷服務攻擊會造成目的IP的服務中斷或網路擁塞。請特別注意:若來源IP為多個且不規則的IP,很可能遭受分散式的阻斷服務攻擊(DDoS)。

處置說明:

- 1.若來源IP數量多、觸發事件數多、持續發生不中斷且造成服務中斷時,請先判斷攻擊流量來源且中斷攻擊來源流量(註:此時阻擋來源IP通常無法有效制止),若攻擊來源為網際網路時,可請ISP協助追查並阻斷攻擊來源。
- 2.若來源IP為內部網路且為特定少數來源IP的SYN FLOOD事件時,請追查為什麼程式或網路路由問題造成。

The '意見記錄' section shows the following information:

- 建立人員:** [Redacted]
- 建立日期:** 2016/03/08 13:03:36
- 審核結果:** 本單位已將本案件處理完畢,並同意結案
- 意見內容:**

老師通知結案:  
內容如下:  
我是 [Redacted],關於上週五(3/4)本校Ip[163.202.305.00]遭通報發生阻斷服務攻擊案件,處理流程與結果如下:

  - 1.將使用該Ip之機台3305-07進行掃毒,未能找到惡意程式。
  - 2.為求保險,已將該機作業系統還原,並更新。
  - 3.加強宣導學生瀏覽安全網頁及不下載安裝不明軟體。

## 二、案件處理(4)

左上角[簽核送單]可輸入簽核意見

The screenshot displays a web browser window with the URL <https://100.72.131.213/Security/Module/Flow/FormDisplay>. The page title is "檢視表單(單號: 794)". The main navigation bar includes "簽核送單" (highlighted), "加會簽", "表單附掛檔案", and "檢視流程".

The form content shows:

- 表單類型: MSS-IDS (資安威脅管理流程)
- 表單狀態: 簽核中
- 關卡抵達時間: 2016-03-09 11:16:45
- 主旨: 第二級[後門/間諜程式行為]案件
- 表單敘述: [1]
- 關卡意義: 通

A modal dialog titled "請輸入簽核意見及決行項目 -- 網頁對話" is open, containing two main sections:

- 簽核意見:** A large empty text area for providing approval comments.
- 決行項目:** A list of action items, with three items highlighted by a red box:
  - 本單位已將本案件處理完畢, 並同意結案
  - 本單位已將本案件處理完畢, 無發現異常並同意結案
  - 請 SOC 人員說明或協助處理本案件

At the bottom of the dialog are buttons for "簽核用語" and "清除".

The sidebar on the left contains a list of case details (表單單號, 案件名稱, 案件方向, 案件狀態, 案件說明) and buttons for "意見記錄", "建立人員", and "簽核結果".

At the bottom of the page, there is a "解決辦法:" section with a partially visible solution: "D... 依佐證資料的時間, 查出惡意查詢之來源IP主機, 通知學校資訊組長協助處理。"

# 三、資產儀表板

點選 [ 資安監控 ] [ 資產儀表板 ] 查訊各校狀況

新北市政府教育局資訊安全整合防護委外服務-SOC服務

歡迎 [ 登入 ]

資產管理 | 歡迎 | 訊息管理 | 資產儀表板

新北教網儀表板-學校端 [ 計時器設定 ]

學校一年內案件列表

ServerName	表單單號	資產警報時間	案件類型	案件名稱	優先性	案件狀態	經過時間	表單敘述
UGuard1	237	2016/02/16 14:49...	Incident	後門/間諜程式行為	第二級	案件成立	000 00:06:01	[163]
UGuard1	236	2016/02/16 14:37...	Incident	後門/間諜程式行為	第二級	案件成立	000 00:07:19	[163]
UGuard1	234	2016/02/16 13:27...	Incident	後門/間諜程式行為	第二級	案件成立	000 00:09:28	[163]
UGuard1	208	2016/01/29 11:28...	Incident	後門/間諜程式行為	第二級	案件成立	000 00:05:56	[163]
UGuard1	207	2016/01/29 11:09...	Incident	後門/間諜程式行為	第二級	案件成立	000 00:16:20	[163]
UGuard1	140	2016/01/13 16:38...	Incident	防火牆分散式服...	第二級	案件處理中	055 19:00:27	[163]
UGuard1	138	2016/01/13 15:57...	Incident	防火牆分散式服...	第二級	案件處理中	055 19:41:16	[163]
UGuard1	136	2016/01/13 15:11...	Incident	防火牆分散式服...	第二級	案件處理中	055 20:27:44	[163]
UGuard1	123	2016/01/12 15:26...	Incident	後門/間諜程式行為	第二級	案件處理中	056 20:12:32	[163]
UGuard1	114	2016/01/12 11:21...	Incident	防火牆分散式服...	第二級	案件處理中	057 00:17:18	[163]

防毒報告列表

事件發生時間	School	InfectedHostIP	VirusInfo	VirusStatus	被封鎖IP列表																																												
沒有任何資料					<table border="1"> <thead> <tr> <th>BlockedDate</th> <th>School</th> <th>BlockedIP</th> <th>IsUnBloc</th> </tr> </thead> <tbody> <tr> <td>2016/02/16 14:49:58</td> <td>國中</td> <td>10.1.1.88</td> <td>Yes</td> </tr> <tr> <td>2016/02/16 14:40:28</td> <td>國中</td> <td>10.1.1.88</td> <td>Yes</td> </tr> <tr> <td>2016/02/16 14:30:12</td> <td>國中</td> <td>10.1.1.88</td> <td>Yes</td> </tr> <tr> <td>2016/02/16 13:33:49</td> <td>國中</td> <td>10.1.1.88</td> <td>Yes</td> </tr> <tr> <td>2016/02/16 13:21:02</td> <td>國中</td> <td>10.1.1.88</td> <td>Yes</td> </tr> <tr> <td>2016/01/29 11:40:32</td> <td>國中</td> <td>10.1.1.88</td> <td>Yes</td> </tr> <tr> <td>2016/01/29 11:28:58</td> <td>國中</td> <td>10.1.1.88</td> <td>Yes</td> </tr> <tr> <td>2016/01/29 11:13:03</td> <td>國中</td> <td>10.1.1.88</td> <td>Yes</td> </tr> <tr> <td>2016/01/29 11:01:52</td> <td>國中</td> <td>10.1.1.88</td> <td>Yes</td> </tr> <tr> <td>2016/01/12 15:01:16</td> <td>國中</td> <td>10.1.1.88</td> <td>Yes</td> </tr> </tbody> </table>	BlockedDate	School	BlockedIP	IsUnBloc	2016/02/16 14:49:58	國中	10.1.1.88	Yes	2016/02/16 14:40:28	國中	10.1.1.88	Yes	2016/02/16 14:30:12	國中	10.1.1.88	Yes	2016/02/16 13:33:49	國中	10.1.1.88	Yes	2016/02/16 13:21:02	國中	10.1.1.88	Yes	2016/01/29 11:40:32	國中	10.1.1.88	Yes	2016/01/29 11:28:58	國中	10.1.1.88	Yes	2016/01/29 11:13:03	國中	10.1.1.88	Yes	2016/01/29 11:01:52	國中	10.1.1.88	Yes	2016/01/12 15:01:16	國中	10.1.1.88	Yes
BlockedDate	School	BlockedIP	IsUnBloc																																														
2016/02/16 14:49:58	國中	10.1.1.88	Yes																																														
2016/02/16 14:40:28	國中	10.1.1.88	Yes																																														
2016/02/16 14:30:12	國中	10.1.1.88	Yes																																														
2016/02/16 13:33:49	國中	10.1.1.88	Yes																																														
2016/02/16 13:21:02	國中	10.1.1.88	Yes																																														
2016/01/29 11:40:32	國中	10.1.1.88	Yes																																														
2016/01/29 11:28:58	國中	10.1.1.88	Yes																																														
2016/01/29 11:13:03	國中	10.1.1.88	Yes																																														
2016/01/29 11:01:52	國中	10.1.1.88	Yes																																														
2016/01/12 15:01:16	國中	10.1.1.88	Yes																																														

Windows Taskbar: 上午 11:39 2016/3/9

# 四、資安新聞

點選[資安監控][資安新聞台]查最新資安新聞

The screenshot shows a web browser window displaying the XFTAS (Xinpei Threat Assessment System) portal. The browser address bar shows the URL <https://soc.ntpc.edu.tw/>. The page title is "新北市府教育局資訊安全整合防護委外服務-SOC服務".

In the left-hand navigation menu, two items are highlighted with red boxes and numbered:

1. 資安監控 (Security Monitoring)
2. 資安新聞台 (Security News Center)

The main content area displays the "XFTAS Daily Threat Assessment for 2016/3/4". It features a section for "每日分析" (Daily Analysis) with a list of links to previous assessments:

- XFTAS Daily Threat Assessment for 2016/3/4
- XFTAS Daily Threat Assessment for 2016/3/03
- XFTAS Daily Threat Assessment for 2016/3/02
- XFTAS Daily Threat Assessment for 2016/3/01
- XFTAS Daily Threat Assessment for 2016/2/29

Below this is a "弱點警報" (Vulnerability Alerts) section listing several CVEs:

- Google Chrome Pdfium JPEG2000越界讀取程式碼執行漏洞(CVE-2016-1628)
- Cisco NX-OS Software拒絕服務漏洞(CVE-2015-6260)
- OpenSSL BIO \*printf函數內存破壞漏洞(CVE-2016-0799)
- phpMyAdmin SQL解析器XSS漏洞(CVE-2016-2559)
- Wireshark ASN.1 BER解析器拒絕服務漏洞(CVE-2016-2522)

Other sections include "病毒智庫" (Virus Knowledge Base) and "病毒警報" (Virus Alerts), each with a list of items and a "More.." link.

On the right side of the page, there is a sidebar titled "資安新聞" (Security News) with a list of links: 每日分析, 弱點警報, 病毒智庫, 病毒警報, 產品更新, 資安新聞, 資安警報.

## 五、Q&A

簡報完畢  
恭請指導

