

## 網路資安日誌平台



### 商品介紹

Zyxel Cyber Security 平台是一款經由 syslog 協定, 自動蒐集數據, 使用瀏覽器即可便利使用, 介面簡潔, 提供容易瞭解的 syslog 分析統計, 具備自訂能力的警報系統及可視化的網路威脅, 讓管理人員洞察先機, 及早處理, 從安全設備安全日誌匯總數據分析和報表。

### 商品特色

1. 自訂重要圖表顯示首頁
2. 集中式資安訊息收集平台
3. 提供豐富多樣的流量圖表
4. 提供資安事件分析
5. 有豐富的即時報表
6. 可以排程報表發送
7. 可顯示系統資源狀態資訊
8. 支援不同管理者帳號

## 流量圖表



## 及時報表與派送

**Dashboard / [Zyxel ATP] - Bandwidth Analysis**

Search... (e.g. status209 AND extension (H/I))

Buttons: **Create Report Now**, **Add Schedule**

Report Name: Weekly\_Bandwidth\_Analysis

Group: None

Periodic: Weekly | Sunday

Mail Configuration:

- Sender: sender@mail.com.tw
- Receiver: receiver@mail.com.tw
- Subject: [Empty]
- Description in Mail Content: [HTML tag]
- Subject Content Parameter: hostname: [HOSTNAME], group name: [GROUP NAME]

## 排程派送

**Report Group SMTP**

Schedule Name	Group
Zyxel_ATP_Performance_Statistics_Last day	none
Zyxel_ATP_Resource_Usage_Summary_Last day	none
Zyxel_ATP_Security_Analysis_Last day	none
Zyxel_ATP_Bandwidth_Analysis_Last day	none

**Schedule**

Report Name: [Text Field]

Group: [Dropdown Menu]

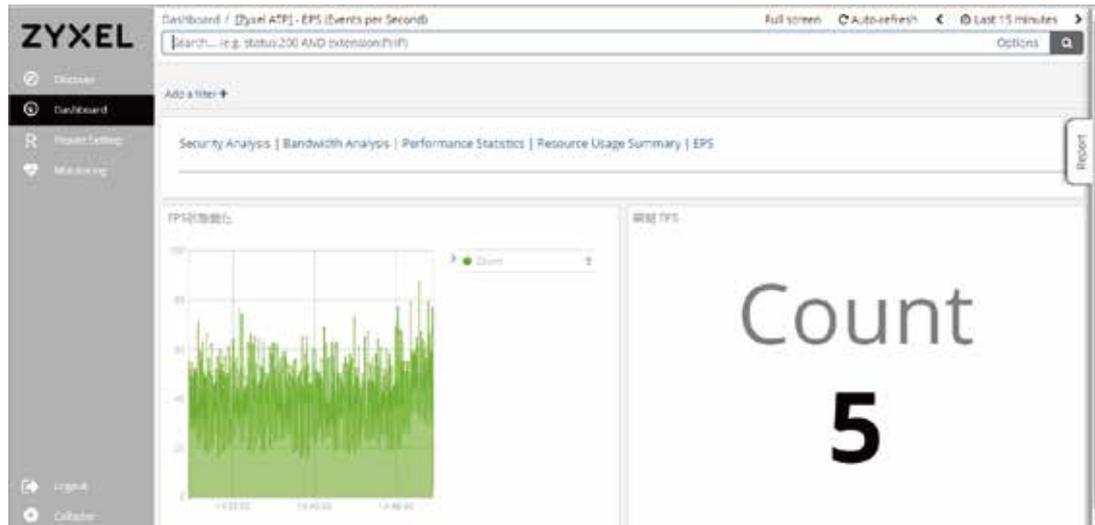
Periodic: [Dropdown Menu] Weekdays: [Dropdown Menu] Time: [Time Picker]

Sender: [Text Field]

Receiver: [Text Field]

Subject: [Text Field]

## 資安事件分析



## 資安訊息收集

The screenshot displays the Malware Detected section of the ZYXEL dashboard. It contains two tables: 'Malware Detected' and 'Malware Source'. The 'Malware Detected' table lists three entries with their device names, virus names, and counts. The 'Malware Source' table lists the source IP addresses for each detected virus.

Device Name	Virus	Count
atp200_101	Malicious Virus	3
atp200_101	EMCAR.Test.File	4
atp200_101	Email-Worm.Win32.Rainouze.b	3

Hostname	Virus	Source IP	Count
atp200_101	Malicious Virus	192.168.101.251	4
atp200_101	EMCAR.Test.File	192.168.101.251	4
atp200_101	Email-Worm.Win32.Rainouze.b	192.168.101.251	3

## 資源狀態

