



**invisiron<sup>®</sup>**

**Cyber**   
**Defence**  
**Fortified<sup>™</sup>**

# 常見資安防禦

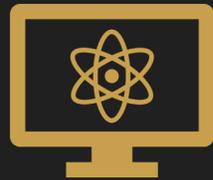
2000y



Now



惡意軟體掃描



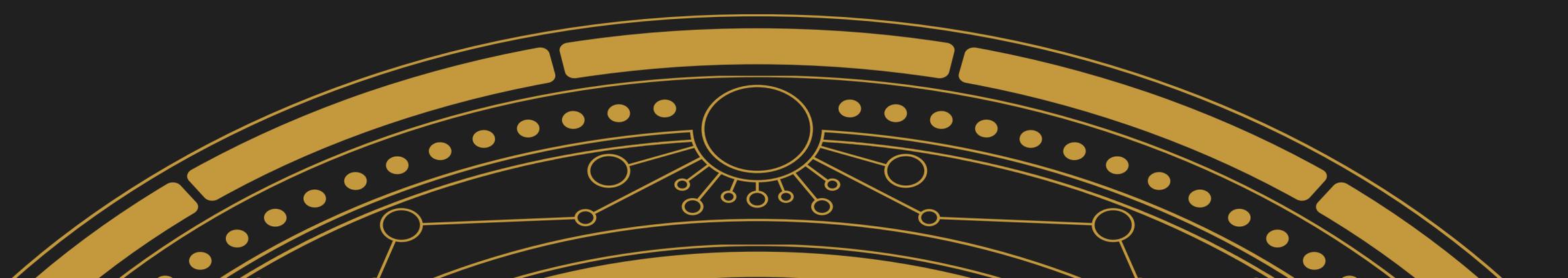
入侵防禦系統



入侵偵測系統



威脅自動防禦系統



# Invisiron 誘捕系統部署區域

有一些攻擊者會特別在當地運作以避免被發現。所以 Invisiron 計劃在全球各地都部署誘捕系統來收集各個地區的網路威脅情資。

目前已經在運作的區域有：

- 新加坡
- 泰國
- 馬來西亞
- 菲律賓
- 印尼
- 澳洲
- 印度
- 台灣

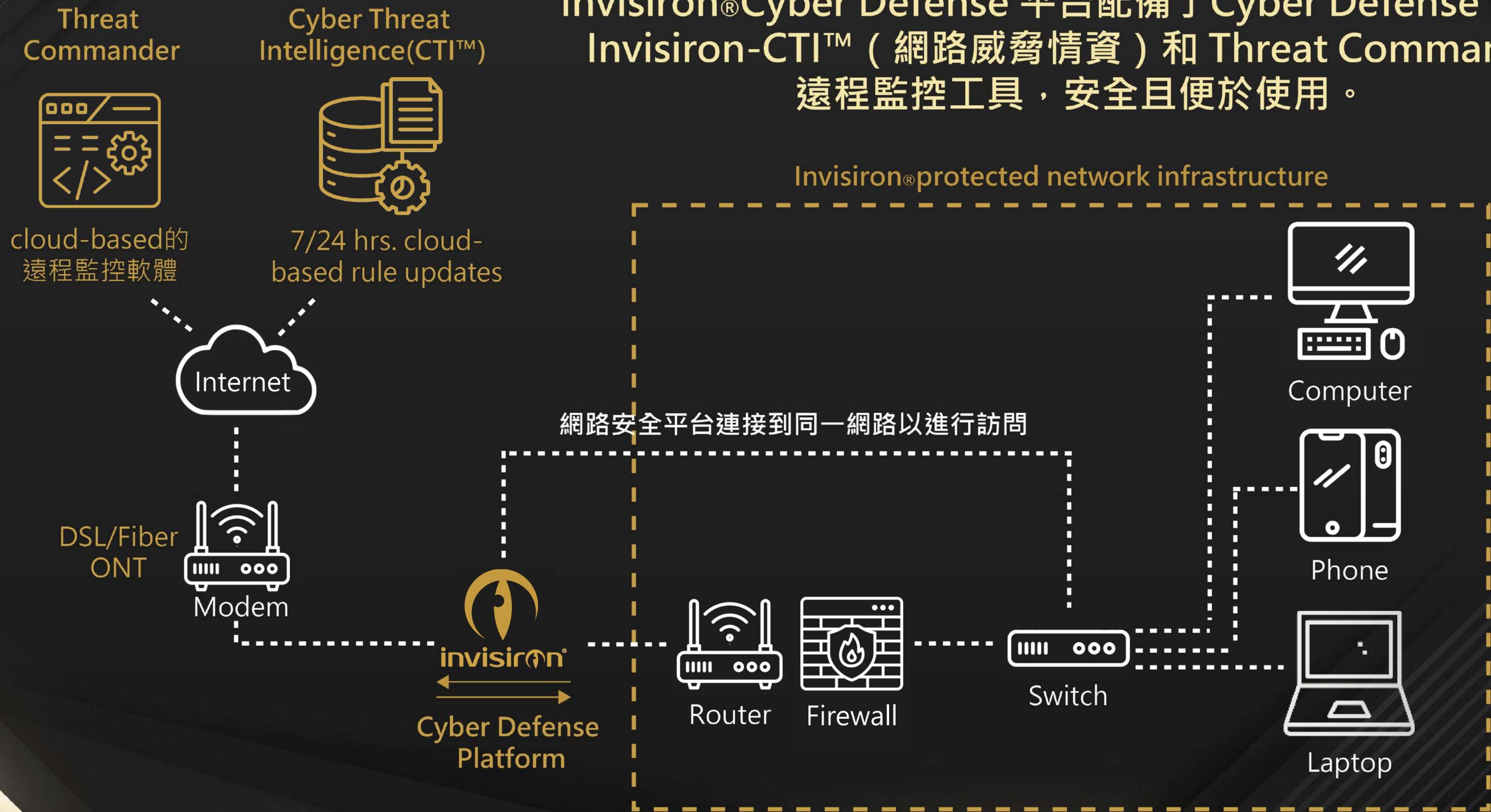
下一階段的區域：

- 中東



# invisiron® 設備配置

Invisiron® Cyber Defense 平台配備了 Cyber Defense 設備、Invisiron-CTI™ (網路威脅情資) 和 Threat Commander 遠程監控工具，安全且便於使用。





# Threat Commander Dashboard

透過驗證和日誌文件管理提供完整的監控功能

Dashboard interface showing navigation menu, Groups table, and event counts.

Ver 3.1 demo

### Groups

Refresh

	CRITICAL	MEDIUM	LOW
InvisironDemo	0	3644	45347

DEVICES	STATUS	HEALTH	THREAT INTEL	MODEL	IDENTIFIER	VERSION	HA MODE	LICENSE
Invisiron777	ONLINE	OK	OK	S-1000	1048697c	3.10.0		2024-09-3

Event Count Summary:

- Critical Severity Event Count: 0
- Medium Severity Event Count: 3644
- Low Severity Event Count: 45347

EVENT LOG | Invisiron777 (1048697c) Ver 3.1 demo

THREAT COMMANDER

DASHBOARD

EXECUTIVE REPORT

CYBER THREAT MAP

EVENTS

EVENT LOG

EVENT CHARTS

TRAFFIC GRAPHS

ANALYTICS

All Events Critical Medium 1 day From 24/11/2022 00:00:00 To 24/11/2022 23:59:59 Refresh Export

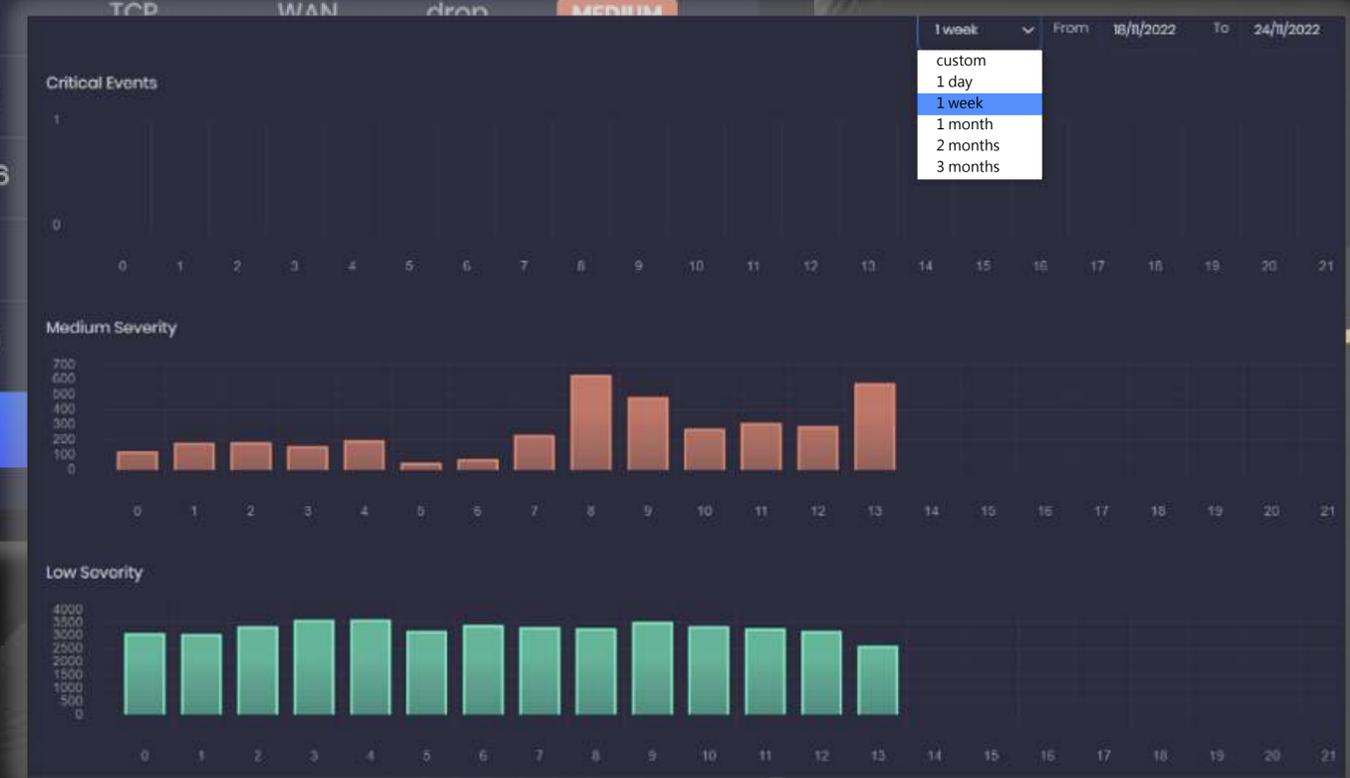
Low URL Block IP Block

Rule Hits

DATE	TIME	RULE ID	MESSA...	SRC IP	SRC PORT	DST IP	DST PORT	PROTOCOL	SOURCE	ACTION	SEVERITY
2022-11-24	13:42:01	110019	+					UDP	WAN	drop	LOW
2022-11-24	13:42:01	100002014	+					TCP	WAN	drop	MEDIUM
2022-11-24	13:41:59	110019	+	118.107.246.2...	443	110.158.43	1900				
2022-11-24	13:41:57	10011	+	146.88.240.4	42484	110.158.43	27016				
2022-11-24	13:41:57	120000	+	182.43.254.1...	53934	110.158.43	25				
2022-11-24	13:41:55	110019	+	118.107.246.2...	443	110.158.43	1900				

< First < Previous 6 rows

IP address scanning for SSDP servers, Possible DDoS use



ATTACK FORENSICS
OB-1000-PemimpinHQ-SingTel02 (f04cd0)
Ver 1.8 ⚙️ johan

- 🏠
- 📄
- 📊
- 🌐
- ☰
- ↕️
- 📄
- STATS
- GEOIP
- FRSC
- SNAP
- 📄
- 📊
- ☰

Attacker IP Anal

134.209.247.16

1 day

Reverse DNS lo

DATE	TIM											COUNTRY NAME	SEVERITY
2021-07-05	12:3											Germany	LOW
2021-07-05	10:2											Germany	LOW
2021-07-05	10:3											Germany	LOW
2021-07-05	10:3											Germany	LOW
2021-07-05	10:3											Germany	LOW
2021-07-05	10:3											Germany	LOW
2021-07-05	10:3											Germany	LOW
2021-07-05	10:3											Germany	LOW
2021-07-05	10:3											Germany	LOW
2021-07-05	09:3											Germany	LOW
2021-07-05	09:3											Germany	LOW
2021-07-05	07:26:09	Honeytrap_T	+ IP blacklisted by: Honeytrap_T	134.209.247.16	41081	42.61.102.211	8132	6	WAN	drop		Germany	LOW

Previous
Page 1 of 3
10 rows
Next

Attacker IP Anal

134.209.247.16

1 day

Reverse DNS lo

DATE	TIM											COUNTRY NAME	SEVERITY
2021-07-05	12:3											Germany	LOW
2021-07-05	10:2											Germany	LOW
2021-07-05	10:3											Germany	LOW
2021-07-05	10:3											Germany	LOW
2021-07-05	10:3											Germany	LOW
2021-07-05	10:3											Germany	LOW
2021-07-05	10:3											Germany	LOW
2021-07-05	10:3											Germany	LOW
2021-07-05	10:3											Germany	LOW
2021-07-05	09:3											Germany	LOW
2021-07-05	09:3											Germany	LOW
2021-07-05	07:26:09	Honeytrap_T	+ IP blacklisted by: Honeytrap_T	134.209.247.16	41081	42.61.102.211	8132	6	WAN	drop		Germany	LOW

Previous
Page 1 of 3
10 rows
Next

Attacker IP Anal

134.209.247.16

1 day

Reverse DNS lo

DATE	TIM											COUNTRY NAME	SEVERITY
2021-07-05	12:3											Germany	LOW
2021-07-05	10:2											Germany	LOW
2021-07-05	10:3											Germany	LOW
2021-07-05	10:3											Germany	LOW
2021-07-05	10:3											Germany	LOW
2021-07-05	10:3											Germany	LOW
2021-07-05	10:3											Germany	LOW
2021-07-05	10:3											Germany	LOW
2021-07-05	10:3											Germany	LOW
2021-07-05	09:3											Germany	LOW
2021-07-05	09:3											Germany	LOW
2021-07-05	07:26:09	Honeytrap_T	+ IP blacklisted by: Honeytrap_T	134.209.247.16	41081	42.61.102.211	8132	6	WAN	drop		Germany	LOW

Previous
Page 1 of 3
10 rows
Next

### Packet Inspection

**Event description:** IP address of known attacker

<b>Ethernet</b>	<b>Source MAC</b> b0:33:a6:90:df:c1	<b>Destination MAC</b> 90:6c:ac:41:bc:5a	<b>Type</b> 0x0800
<b>Header (14) / Payload (46)</b>			
<b>IPv4</b>	<b>Source IP</b> 134.209.247.16	<b>Destination IP</b> 42.61.102.211	<b>Protocol</b> TCP
<b>Header (20) / Payload (26)</b>			
<b>TCP</b>	<b>Source port</b> 52778	<b>Destination Port</b> 8532	<b>Payload size</b> 6
<b>Header (20) / Payload (6)</b>			

**Timestamp**  
Jul 5 2021 10:42:32

**Number of packets**  
1

**Packet displayed**  
← 1 →

**Coloring**  
 OFF  ON

<pre> 0000  90 6c ac 41 bc 5a b0 33  a6 90 df c1 08 00 45 00 0010  00 28 67 6a 00 00 e8 06  5c 73 86 d1 f7 10 2a 3d 0020  66 d3 ce 2a 21 54 ee 3d  20 ed 00 00 00 00 50 02 0030  04 00 9e 46 00 00 6e e3  00 00 00 00                     </pre>	<pre> 0000  . 1 . A . Z . 3 . . . . . E . 0010  . ( g j . . . . \ s . . . . * = 0020  f . . * ! T = . . . . . P . 0030  . . . F . n . . . . .                     </pre>	
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--



ALL TRAFFIC

Invisiron777 (1048697c)

Ver 3.1



demo

TRAFFIC GRAPHS

ALL TRAFFIC

DNS TRAFFIC

ICMP TRAFFIC

SSH TRAFFIC

SBM\_139 TRAFFIC

SMB\_445 TRAFFIC

RDP TRAFFIC

FRAGMENTED PACKETS TRAFFIC

1 day



From

24/11/2022

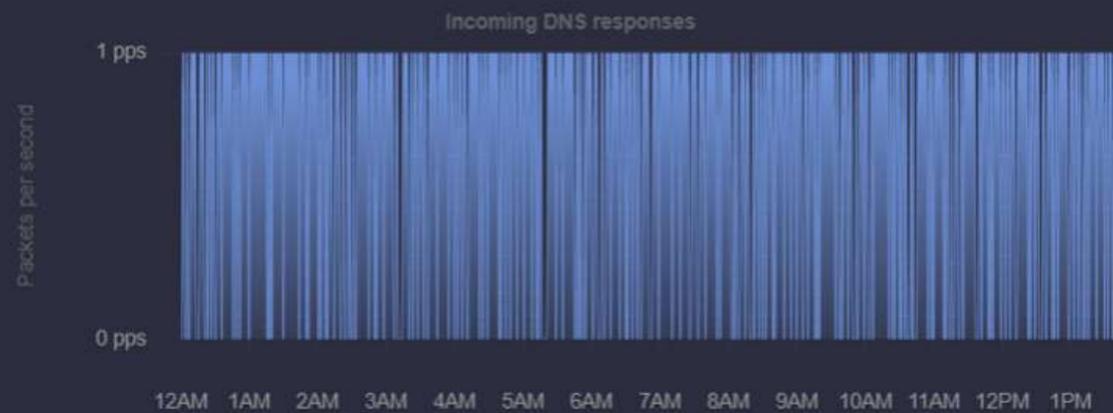
To

24/11/2022

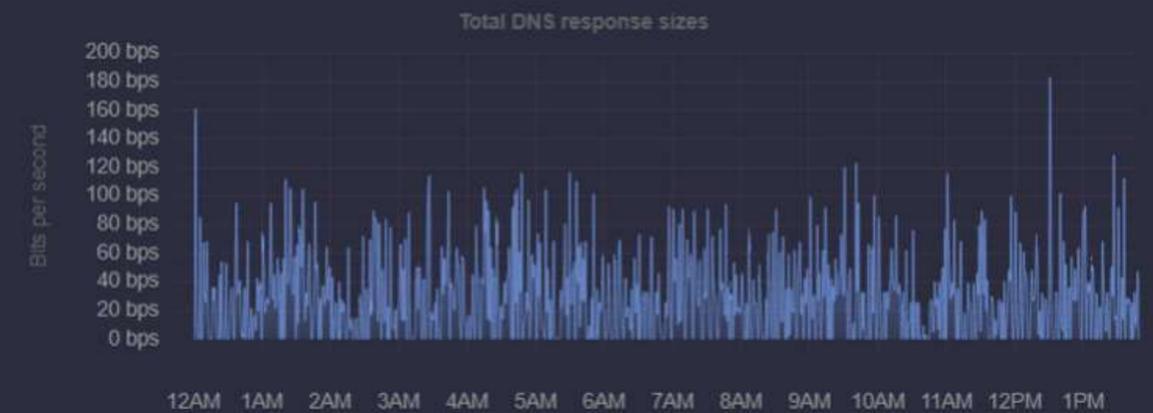


Refresh

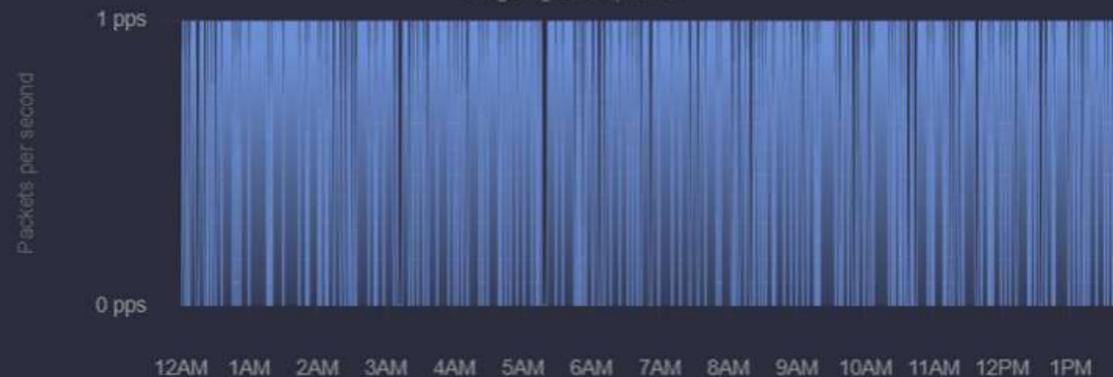
DNS Query and Response Traffic



DNS Response Traffic Statistics

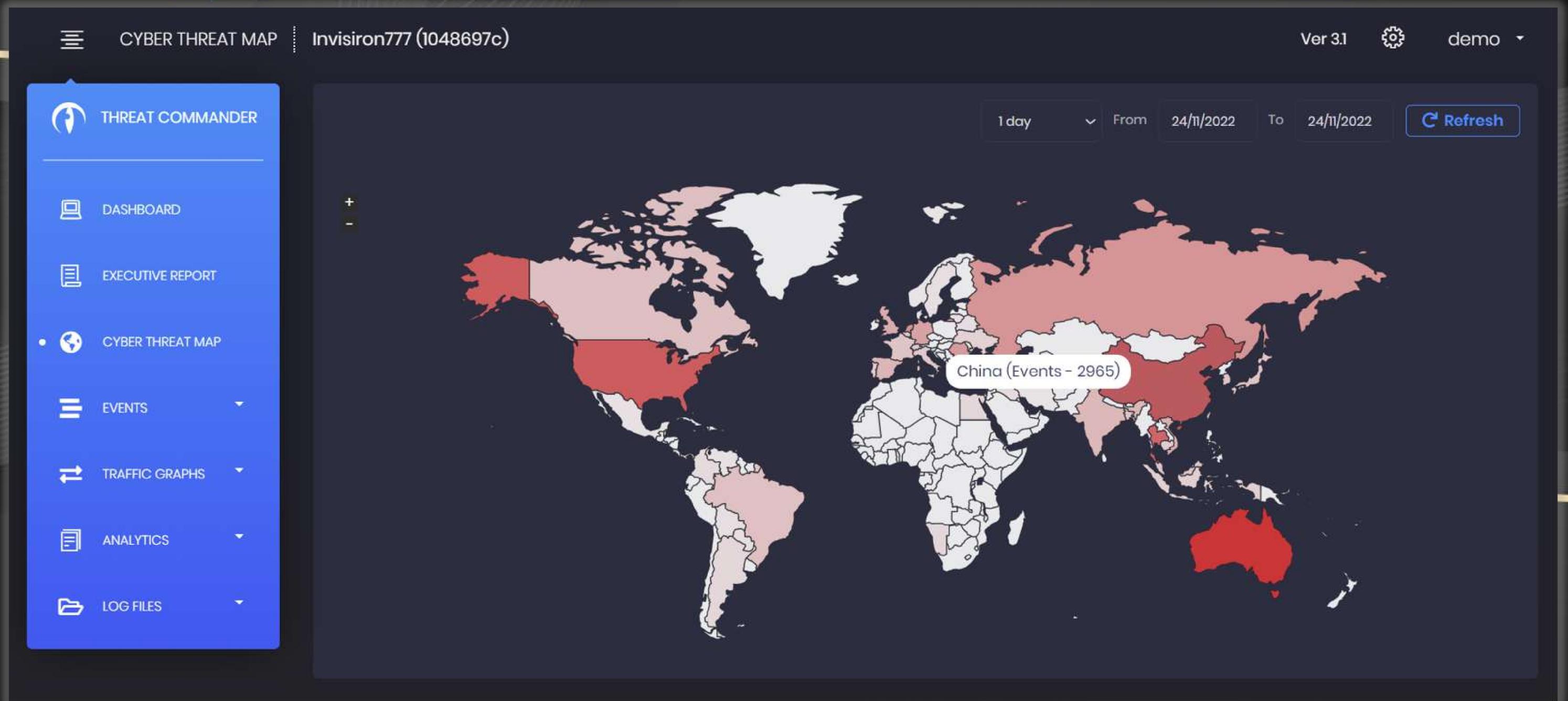


Outgoing DNS queries



Incoming DNS NXDOMAIN responses







# ELOGY TAIWAN

台灣特洛奇資訊有限公司

886-2-22266269

Email : [sales@telogy.com.tw](mailto:sales@telogy.com.tw)

<http://www.telogy.com.tw>

23586 新北市中和區中正路920號7樓

**invisiron**<sup>®</sup>