



臺灣資安大會
CYBERSEC 2019

IT人轉職資安人的起手式

博格企業資安讀書會 創辦人 X1

About Me

社群代號:

資安黑武士 / X1

社群經歷:

博格企業資安讀書會 創辦人

中華民國無店面零售商業同業公會 - 資安防護講座講師

TDOH 2017 - 反抗無用，接受進步 (北韓惡意樣本分析)

TDOH 2018 - 企業防禦 DDoS 方式與探討 – 工作坊講師

HITCON Defense 2018 技術總招

聲明

想分享一切所知卻受束縛的資安人，深怕打開潘朵拉盒子，引起殺生之禍
/ 查水表 / 歡樂送 / 失業，只能蒙上面具，以黑武士奉獻自己的淺學

本人對外之言行及演講內容均與本人服務公司無關，亦不代表公司立場

議程

- 本議程適用對象&目標
- 資安問題怎麼辦？
- 問題討論(Q&A)

議程





臺灣資安大會
CYBERSEC 2019

本議程適用對象&目標

本議程適用對象



IT人轉職資安人



中小企業主



預算有限的朋友

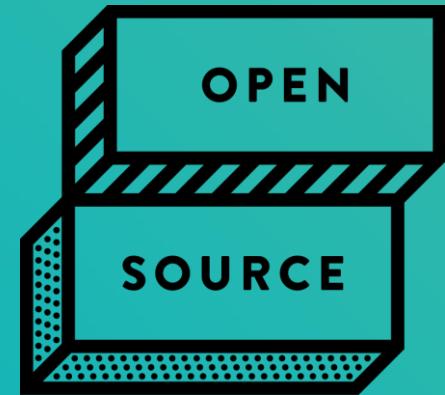
本議程目標



How to start



搜索簡報的關鍵字



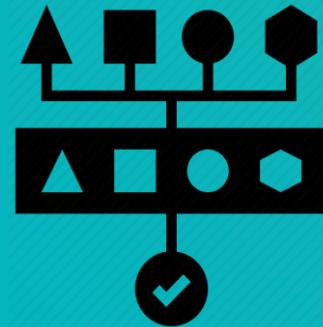
低預算也很安全

特別注意的風險 !!

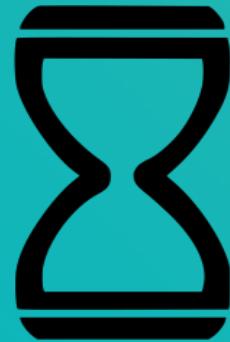
Open Source 和 商用付費還是有差異的 !!



壞了要自己修



自己的資料自己分析



花時間研究和部署



更新與相容問題



臺灣資安大會
CYBERSEC 2019

資安問題怎麼辦？

資安問題怎麼辦？

事前

- 所有資產做過資安盤點了嗎？
- Internet出入口/雲端服務 如何整合、管制？
- 到底開了多少對外服務？
- 是否都更新了？
- 我的伺服器在幹嘛？有人登入了？

事中

- 網站DDoS翻了，怎麼辦
- 我的網站是破口嗎？
- 被入侵！馬上重灌？

事後

- 資安事件處理、通報，做到位了嗎？
- 防毒軟體防不了駭，怎麼辦？
- 未收集的AP/DB Log如何補救？

資安問題怎麼辦？

硬體 : OCS Inventory – 記錄所有用戶以利資安盤點

資安問題怎麼辦？

OCS Inventory NG Ver. 2.1.2

硬

The screenshot shows the OCS Inventory NG software interface. At the top, there are several blue circular icons representing different asset types: server, network, storage, print, and search. To the right are yellow circular icons for various management functions like backup, monitoring, and reporting. The top right corner displays the version "Ver. 2.1.2". Below the header is a toolbar with buttons for file operations. The main area features a table titled "1927 Result(s) (Download)". The table has columns for Account info, Last inventory, Computer, User, Operating system, RAM (MB), CPU (MHz), Select, and Delete. Each row contains information about a specific computer asset, such as its name, last inventory date, operating system, and hardware specifications. The "Select" column contains checkboxes, and the "Delete" column contains red X icons.

Account info: TAG	Last inventory	Computer	User	Operating system	RAM (MB)	CPU (MHz)	Select	Delete
Biblioteca Piso 1	2015-11-18 10:55:25	CU	UnisabanaIT	Microsoft Windows 7 Professional	3241	2601	<input type="checkbox"/>	X
Punto pago 1	2015-11-18 10:55:06	PORT-PRESADM154	presadmin54	Microsoft Windows 7 Professional	6662	2401	<input type="checkbox"/>	X
Punto pago 1	2015-11-18 10:53:56	PORT-PRESADM144	presadmin144	Microsoft Windows 7 Professional	6662	2401	<input type="checkbox"/>	X
Mesón	2015-11-18 10:53:49	CU-PAUTOSERV2	Pautoserv2	Microsoft Windows 7 Professional	3072	3200	<input type="checkbox"/>	X
Mesón	2015-11-18 10:53:43	CU-PCAFE2	Pverde2	Microsoft Windows 7 Professional	1790	3200	<input type="checkbox"/>	X
Facultad de Educación	2015-11-18 10:53:01	PORT-COORDMAE	coordinacionmae	Microsoft Windows 7 Professional	3298	2501	<input type="checkbox"/>	X
Edificio F Salones	2015-11-18 10:52:54	CUFA204F01		Microsoft Windows 7 Professional	3072	3200	<input type="checkbox"/>	X
Instituto de Posgrados FORUM	2015-11-18 10:52:54	S80-JOHNNATHAND	sandraroca	Microsoft Windows 7 Professional	3543	3000	<input type="checkbox"/>	X
EICEA	2015-11-18 10:52:51	PORT-IVANGD	Ivangd	Microsoft Windows 7 Professional	4096	2501	<input type="checkbox"/>	X
Studium	2015-11-18 10:52:43	LE-NOVACK3	studium	Microsoft Windows 7 Professional	3416	3401	<input type="checkbox"/>	X
Punto pago 1	2015-11-18 10:52:37	PORT-PRESADM121	presadmin121	Microsoft Windows 7 Professional	6662	2401	<input type="checkbox"/>	X
Dirección Financiera	2015-11-18 10:52:30	CU-CARLOSBA	aureliodeve	Microsoft Windows 8 Pro	6144	3201	<input type="checkbox"/>	X
Dirección Central de Estudiantes	2015-11-18 10:51:58	PORT-CARLOSMOJI	carlosmoji	Microsoft Windows 7 Professional	6662	2401	<input type="checkbox"/>	X
Facultad de Medicina	2015-11-18 10:51:11	CLI-JULIOML	julioml	Microsoft Windows 7 Professional	3543	3000	<input type="checkbox"/>	X
Relaciones Internacionales	2015-11-18 10:49:43	CU-OFFICINA	fabianmega	Microsoft Windows 10 Pro	3072	3200	<input type="checkbox"/>	X
Edificio G Salones	2015-11-18 10:48:47	CUGA217F01	CUGA217F01	Microsoft Windows 7 Professional	3072	3200	<input type="checkbox"/>	X
Punto pago 1	2015-11-18 10:48:40	PORT-PRESADM99	presadmin99	Microsoft Windows 7 Professional	6662	2401	<input type="checkbox"/>	X

資安問題怎麼辦？

網路邏輯 : The Dude 盤點自己的網路

資安問題怎麼辦？

網路遜

10.5.104.0/24 - Network Map

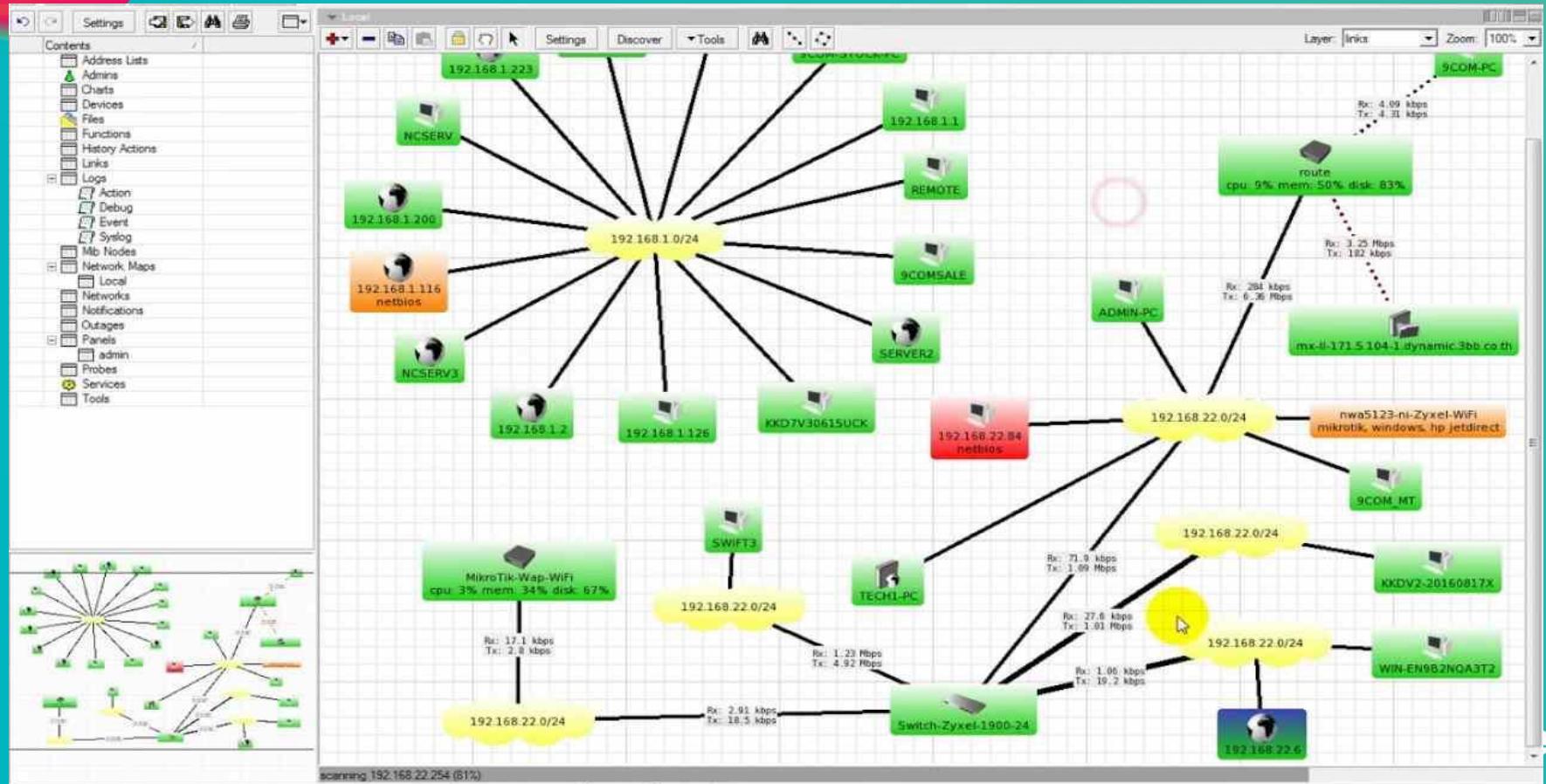
General Polling Outages Appearance Background Export

Remove Resolved Status: all Device: all Service: all

	Status	Time	Duration	Device	Service	
1	active	Dec/16 12:49:17	2d 04:39:25	gateway.lan	dns	
2	active	Dec/16 12:49:17	2d 04:39:25	gateway.lan	radius	
3	active	Dec/16 12:49:16	2d 04:39:26	gateway.lan	router	
4	active	Dec/16 12:49:16	2d 04:39:26	gateway.lan	mikrotik	
5	active	Dec/16 12:49:16	2d 04:39:26	gateway.lan	switch	
6	active	Dec/16 12:49:07	2d 04:39:35	gateway.lan	disk	
7	active	Dec/16 12:49:07	2d 04:39:35	gateway.lan	cpu	
8	resolved	Dec/16 15:06:42	00:00:16	crs212.lan	ssh	
9	resolved	Dec/16 15:06:42	00:00:16	crs212.lan	http	
10	resolved	Dec/16 15:06:42	00:00:17	crs212.lan	ftp	
11	resolved	Dec/16 15:06:41	00:00:17	crs212.lan	ping	
12	resolved	Dec/16 15:03:57	00:00:32	crs212.lan	ftp	
13	resolved	Dec/16 15:03:57	00:00:32	crs212.lan	http	
14	resolved	Dec/16 15:03:57	00:00:31	crs212.lan	ssh	
15	resolved	Dec/16 15:03:56	00:00:32	crs212.lan	ping	
16	resolved	Dec/02 11:22:46	00:03:00	crs226.lan	http	
17	resolved	Dec/02 11:22:46	00:03:00	crs226.lan	ssh	
18	resolved	Dec/02 11:22:46	00:03:27	crs226.lan	ping	
19	resolved	Dec/02 11:22:46	00:03:00	crs226.lan	ftp	
20	resolved	Dec/02 11:22:34	00:03:27	nine.lan	http	
21	resolved	Dec/02 11:22:34	00:03:27	nine.lan	ping	
22	resolved	Dec/02 11:22:34	00:03:20	ppc.lan	dns	
23	resolved	Dec/02 11:22:34	00:03:27	nine.lan	telnet	
24	resolved	Dec/02 11:22:34	00:03:27	nine.lan	ssh	
25	resolved	Dec/02 11:22:34	00:03:27	nine.lan	ftp	

Ok Cancel Apply Notes

資安問題怎麼辦？



資安問題怎麼辦？

評估資安風險 – 範例表單（新竹市稅務局）：

稅務資料處理過程中必須符合機密性、完整性及可用性，為了達到這個目標及降低資訊作業風險，於2009年以專案方式聘請專業講師，教導竹市稅務員工自行建置資訊安全管理制度系統，並將攸關納稅人權益之退稅業務為核心業務納入驗證，進而推動資安治理、制定各項文件等，其中，資訊資產盤點表就是建置ISMS時不可或缺的文件。

引用來源: 資安人

■ a5796.xls [相容模式]

Q 搜尋工作表

常用 插入 頁面配置 公式 資料 校閱 檢視

剪下 複製 格式 新細明體 12 A A = = 自動換行 通用格式 條件式 格式設定 格式化為表格 儲存 格樣式 插入 刪除 格式 自動加總 填滿 清除 排序與篩選

Office Update To keep up-to-date with security updates, fixes, and improvements, choose Check for Updates.

M27 A B C D E F G H I J K L M N O P Q R S T U V W X

1 風險評鑑工作底稿(彙總後)

2

3 資產群組名稱 資產群組編號 資產類別 資產次類別 機密性 完整性 可用性 最大值 風險值

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

32

33

34

35

36

37

38

39

40

41

空白 業務流程與活動 資訊 硬體 軟體 網路 人員 場地 組織活動 彙總1 風險排序 風險排序黑白 最大值排序 風險值分析 風險值統計 +

人

資安問題怎麼辦？

到底開了多少對外服務 – nmap 定期盤點您是否有不知道服務對外？

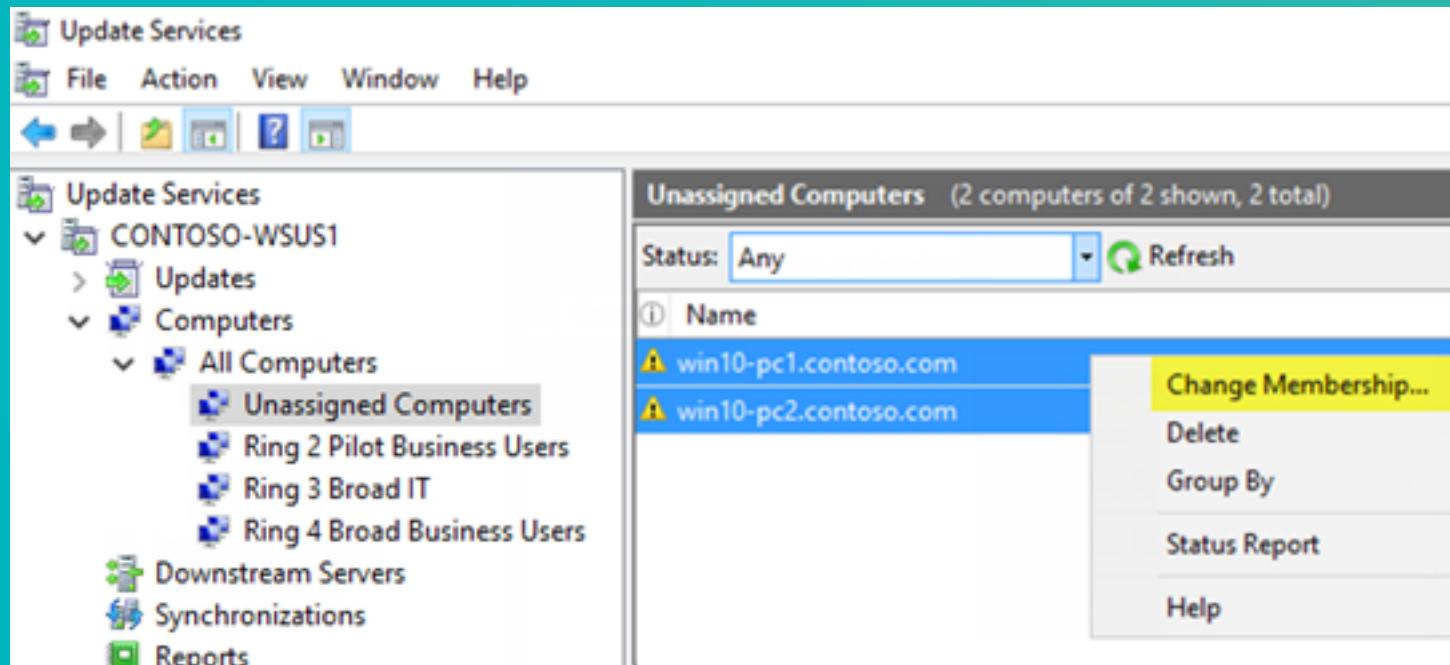
```
# nmap -A -T4 scanme.nmap.org d0ze
Starting Nmap 4.01 ( http://www.insecure.org/nmap/ ) at 2006-03-20 15:53 PST
Interesting ports on scanme.nmap.org (205.217.153.62):
(The 1667 ports scanned but not shown below are in state: filtered)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh    OpenSSH 3.9p1 (protocol 1.99)
25/tcp    open  smtp   Postfix smtpd
53/tcp    open  domain ISC Bind 9.2.1
70/tcp    closed gopher
80/tcp    open  http   Apache httpd 2.0.52 ((Fedora))
113/tcp   closed auth
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.0 - 2.6.11
Uptime 26.177 days (since Wed Feb 22 11:39:16 2006)

Interesting ports on d0ze.internal (192.168.12.3):
(The 1664 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp    Serv-U ftptd 4.0
25/tcp    open  smtp   IMail NT-ESMTP 7.15 2015-2
80/tcp    open  http   Microsoft IIS webserver 5.0
110/tcp   open  pop3   IMail pop3d 7.15 931-1
135/tcp   open  mstask  Microsoft mstask (task server = c:\winnt\system32\
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows XP microsoft-ds
1025/tcp  open  msrpc   Microsoft Windows RPC
5800/tcp  open  vnc-http Ultr@VNC (Resolution 1024x800; VNC TCP port: 5900)
MAC Address: 00:A0:CC:51:72:7E (Lite-on Communications)
Device type: general purpose
Running: Microsoft Windows NT/2K/XP
OS details: Microsoft Windows 2000 Professional
Service Info: OS: Windows

Nmap finished: 2 IP addresses (2 hosts up) scanned in 42.291 seconds
flog/home/fyodor/nmap-misc/Screenshots/042006#
```

資安問題怎麼辦？

是否都更新了？ - WSUS



資安問題怎麼辦？

我的伺服器在幹嘛？有人登入了？

The screenshot shows the Zabbix web interface with the following highlights:

- Monitoring** tab is selected (highlighted by a red box and circled ①).
- Latest data** button is highlighted by a red box and circled ②.
- The **Host groups** search bar contains "Windows-10" (highlighted by a red box and circled ③).
- The **Hosts** search bar contains "Windows-10" (highlighted by a red box and circled ③).
- The **Application** search bar contains "Windows Event Log Monitor" (highlighted by a red box and circled ③).
- The **Apply** button is highlighted by a red box and circled ④.
- In the bottom navigation bar, the "Windows Event Log Monitor" item is highlighted by a red box and circled ④.

The main content area displays the following information for the selected host:

Name	Last check
Windows Event Log Monitor	03/10/2017 04:24:38 PM

At the bottom, there are buttons for "Display stacked graph" and "Display graph".

資安問題怎麼辦？

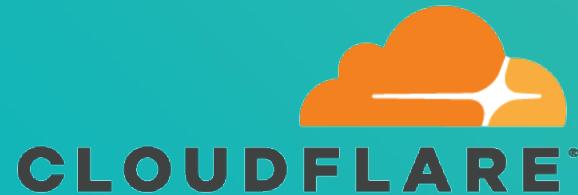
自動化封鎖 - fail2ban/wail2ban

The screenshot shows a Cloudflare error page. At the top, it displays "Error 1006" and "Access denied". Below this, a section titled "What happened?" states: "The owner of this website (technicalramblings.com) has banned your IP address (46.246.123.163)." To the right of the text is a small illustration of a house with a "no entry" sign over it. The Cloudflare logo is prominently displayed at the bottom left, and the text "Cloudflare Ray ID: 46320e83fe4142b5 • 2018-10-01 21:35:01 UTC" is at the bottom center.

https://www.fail2ban.org/wiki/index.php/Main_Page
<https://github.com/glasnt/wail2ban>

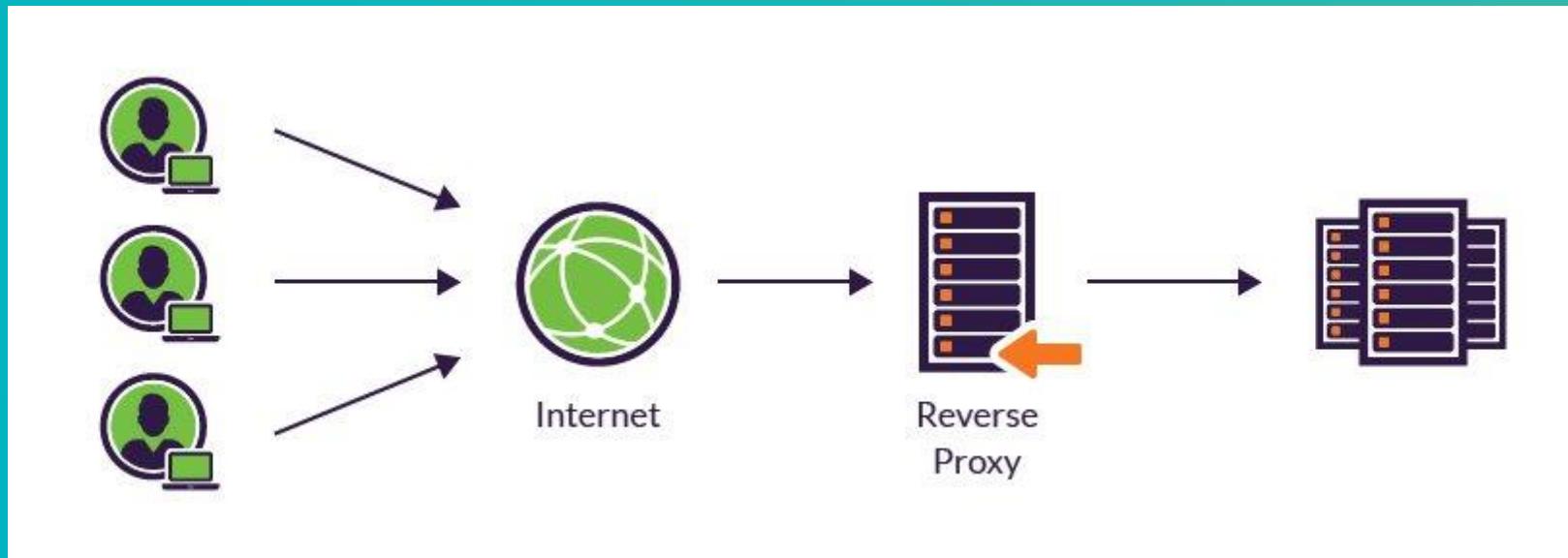
資安問題怎麼辦？

網站DDoS翻了，怎麼辦？



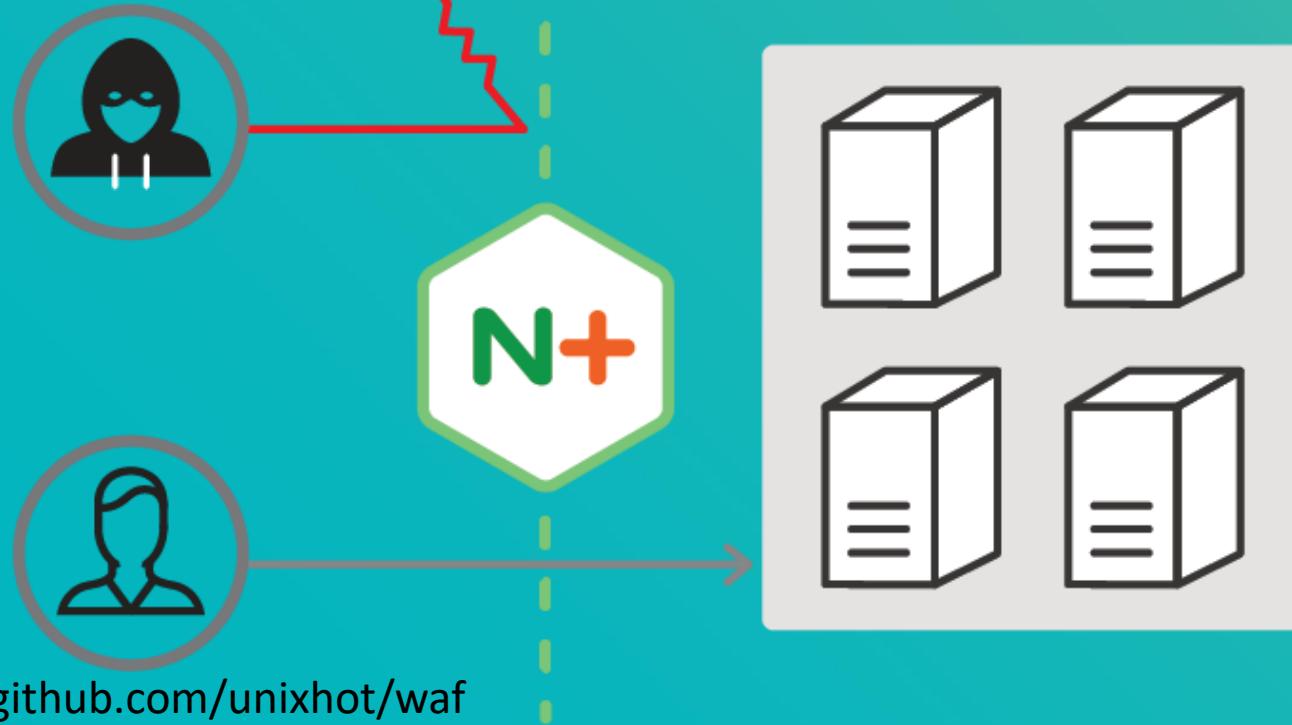
資安問題怎麼辦？

我的網站是破口嗎？ - WAF



WAF – NGINX

<https://www.nginx.com/blog/nginx-plus-r10-released/>



資安問題怎麼辦？



資安問題怎麼辦？



資安問題怎麼辦？

Endian UTM

HTTP

POP3

FTP

SMTP

DNS

HTTP proxy: Authentication

Configuration Access Policy Authentication Web Filter AD join HTTPS Proxy

Choose Authentication Method *
LDAP (v2, v3, Novell eDirectory, AD) ▾

Authentication settings ?

Authentication Realm *
Proxy Server

Number of Authentication Children *
20

Number of different ips per user *
0

Authentication cache TTL (in minutes) *
60

User / IP cache TTL (in minutes) *
0

LDAP specific settings ?

LDAP server *
192.168.6.99

Bind DN settings *
DC=lab03,DC=com

Bind DN username
CN=Administrator,CN=Users,DC=lab03,DC=com

user objectClass *
person

Port of LDAP server *
389

LDAP type *
Active Directory Server ▾

Bind DN password

group objectClass *
group

Save

* This Field is required.

資安問題怎麼辦？

被入侵！馬上重灌？ - 錯！ 數位鑑識包 - Helix





臺灣資安大會

CYBERSEC 2019

Q&A

Q&A ?



<https://t.me/BorgEnt>

社群夥伴



臺灣資安大會

CYBERSEC 2019

PRESENTED BY **iThome**