CYBERSEC 2021
臺灣資安大會

ORGANIZED BY iThome

TRUST:redefined

信 任 重 構

MAY 4-6 臺北南港展覽二館

醫療資安人才困境與應對

粘良祁

彰化基督教醫院 資安長

TRUST: redefined

別人以為

https://kknews.cc/sports/68ypyvp.html

https://www.easyatm.com.tw/wiki/%E7%BE%8E%E5%9C%8B%E9%9A%8A%E9%95%B7

現實中

https://www.mplus.com.tw/article/142

https://opinion.udn.com/opinion/story/8159/1317267

資安專業人才

- 根據大同大學林宜隆教授的分類
- 資安防護人才
- 資安攻擊人才
- 資安鑑識人才
- 資安偵查人才
- 資安教育人才
- 資安治理人才

我國數位鑑識能量規劃與發展現況

@資安專業人才

(DEFSOP=ISO27002+27037+27041+27102+27035)

- 資安防護人才(Q/Y, UNIT,Contents)
- 資安攻擊人才(CIISP,CEH,ISO27005)
- 資安鑑識人才(ACE/EnCE/CFCE/UCE/CFE/CHFI)
- 資安偵查人才(CFCE/CFE,ISO27037,ISO27041-43)
- 資安教育人才(ISO27001/27011 LA,ISO27011,ISO27015)
- 資安治理人才(ISO27014,ISO27017,ISO27701,ISO27102)

關於公部門資安人力配置情形，政院資安處統計，截至今(2020)年6月30日機關填報資安維護計劃統計，資安責任等級C級以上機關共有1330個，填報資料之機關1294個，依法應配置1678名專職人力，目前僅有993人，其中正式職員僅685人，約缺1024名專職人力。綠委質疑部會資安人力竟缺逾千

/2020/12/07

大同大學
林宜隆教授

TRUST: redefined

困境

CYBERSEC 2021
臺灣資安大會

ORGANIZED BY
iThome

缺

TRUST:
redefined

MAY 4-6 臺北南港展覽二館

≡ 經理人

領導帶人 經營管理 行銷業務 工作術 自我管理 專題 近期活動

台積電徵才 9 千人！新鮮人起薪高於業界近 2 倍，將造成其他產業「新人空洞」？

IN 2021/04/01 MindyLi

黑洞效應

台灣資安人才的職涯挑戰

當罰款小於薪資的時候

供需差異 企業是否了解資安業務需求及其對應的人才？資安人才是否有相關背景？

職涯發展 資安人才的職涯有哪些發展可能性？工作內容可否獲得成就感與挑戰性？

薪資落差 資安相關職缺的薪資水準是否有跟上市場的供需機制？

金融業沒喊缺人

人才投資 資安人才的培育和培訓，企業與政府的角色定位為何？

一言不合就被罰款

SECURITY TALENT

2021 資安大會
Enable a Culture-Driven Cybersecurity Transformation in Taiwan
台灣未來基金會 創辦人 陳浩維

NEX FOUNDATION

TRUST: redefined

港 展 覽 二 館

28

熱門職缺含金量Top10

資料來源：104人力銀行

熱門職缺排名	工作內容	平均月薪（元）
資料科學家	將產業相關問題轉為數學問題，設計演算法建立模型，從大數據挖取具商業價值的訊息。	81,902
電腦視覺工程師	負責電腦判別影像處理、演算法與軟體開發，應用領域為健康醫療、安全監控及自駕車等。	71,308
機器學習開發工程師	開發及部署機器學習的預測模型，並進行演算法設計及分析，評估可應用範圍。	70,812
區塊鏈工程師	開發並維護區塊鏈去中心化程式；需涉獵網路架構、資料庫設計及密碼學等。	70,447
DevOps工程師	在軟體團隊中扮演降低開發與營運團隊間隔閡的角色，以提升軟體更新速度及穩定度。	65,728
大數據架構師	規劃及開發大數據收集，[illegible]化並建置成大數據[illegible]。	63,416
全端工程師	網站與App的[illegible]資料庫的設置與[illegible]	55,516
AI專案管理師	負責人工智慧[illegible]具備跨領域[illegible]	54,942
資安工程師	控管資安設備與分析數據、優化資安架構；發生資安事件時，需分析事件及排除問題。	53,713
MES工程師	管理製造流程，並負責[illegible]	[illegible]

45K的例子

https://finance.ettoday.net/news/1948869

彰基資安中心人力

資安中心目前設置1人

專職?

專責?

已應徵近兩年時間，找不到合適資安人員

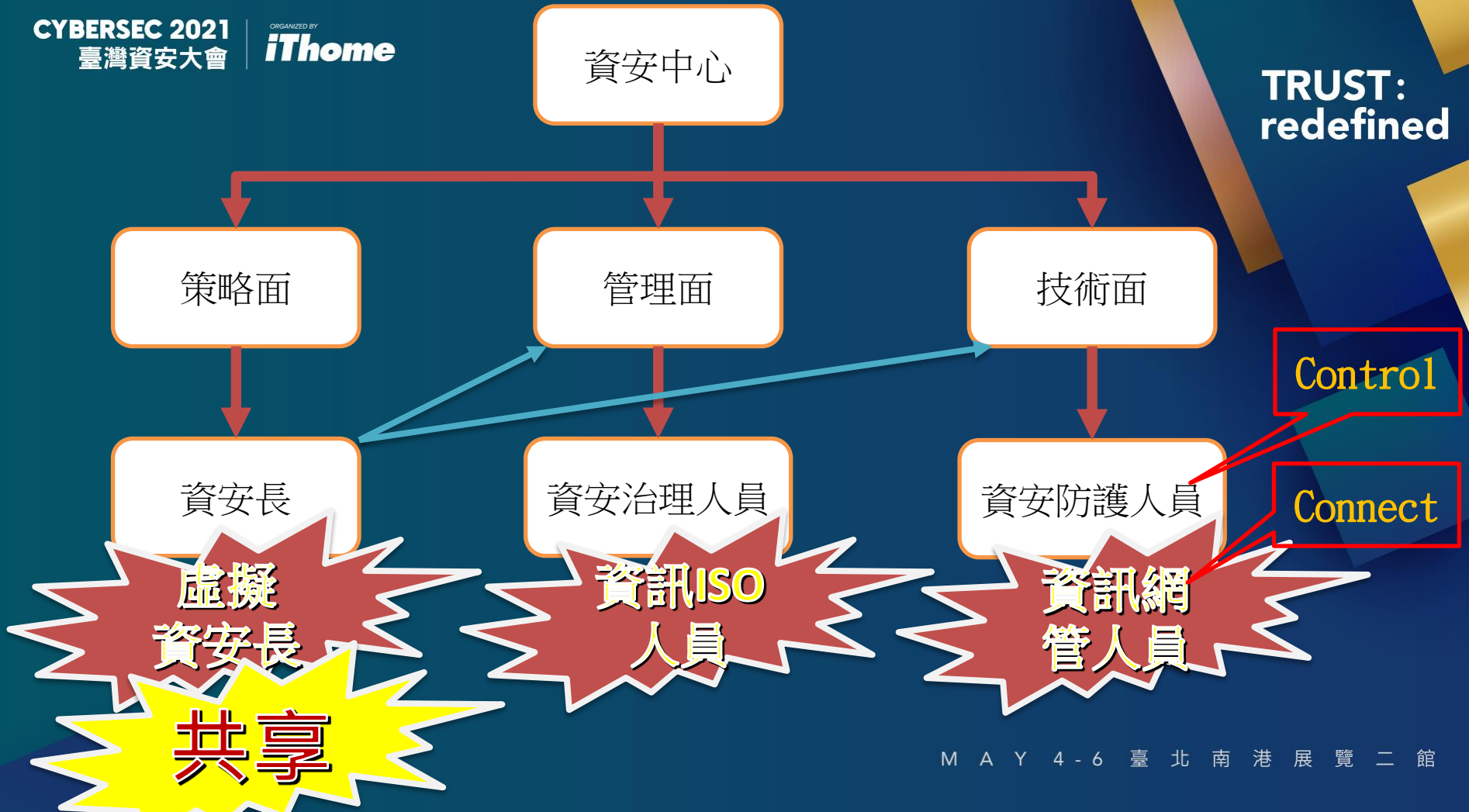
醫療資安三缺困境

- 缺人
- 缺錢
- 缺時間

TRUST: redefined

應對

缺人


資安中心
策略面
管理面
技術面
資安長
資安治理人員
資安防護人員
Control
Connect
虛擬資安長
資訊ISO人員
資訊網管人員
共享

TRUST: redefined

應對

缺錢

訂定中長遠的資安目標

規劃

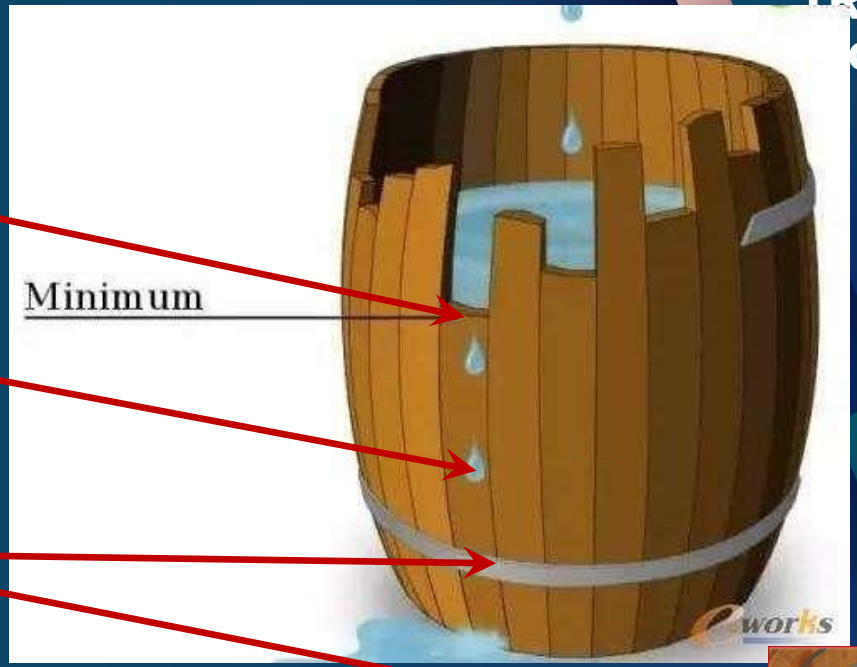
避免無效或
重複的支出

執行

木桶理論

SOC
(Security Operation Center)

資安管理制度並落實



收集Log，網路可視化

https://www.ruten.com.tw/item/show?21942373044032

內網可視化之入門五能心法

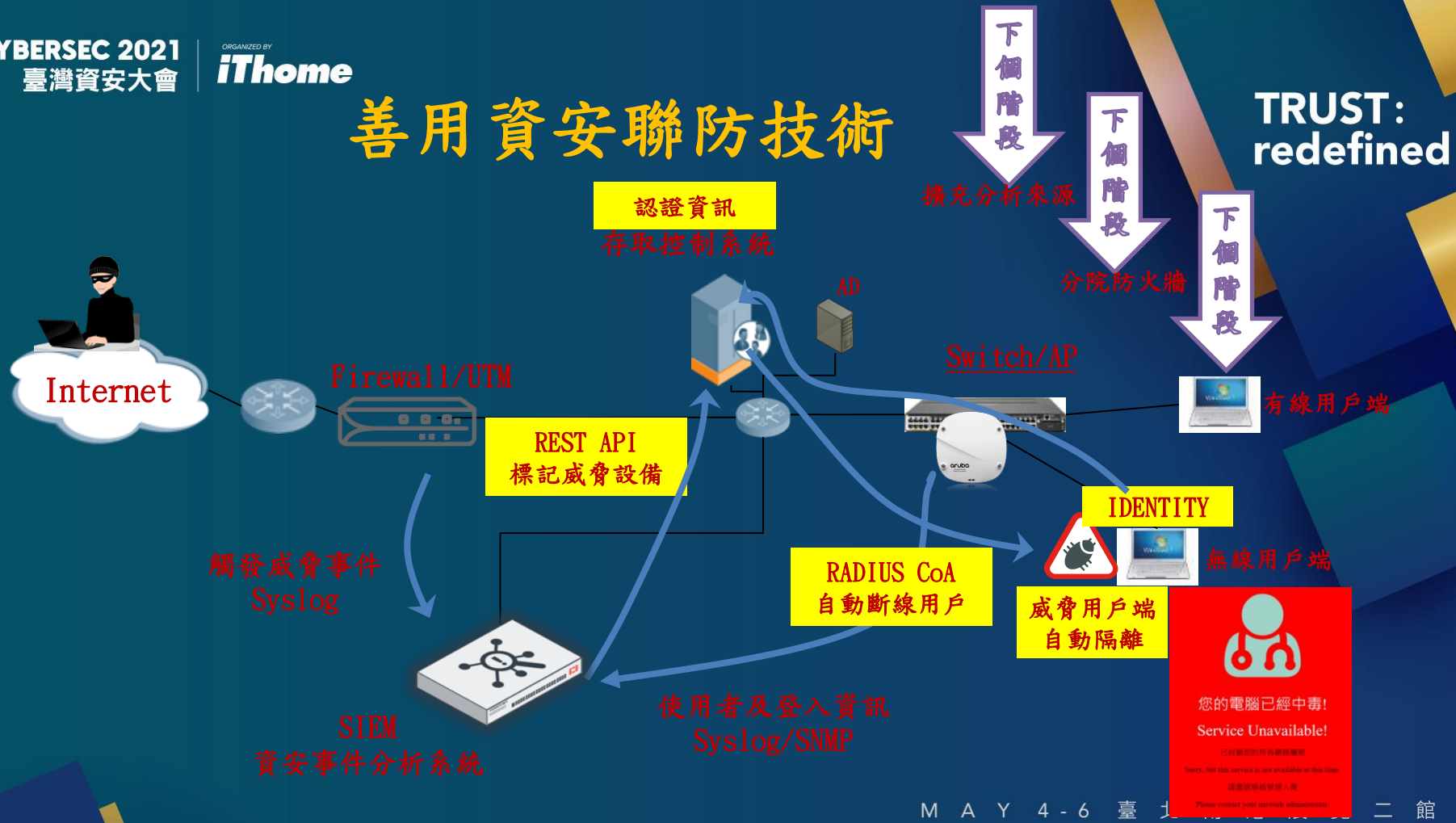
- 所有攻擊行為都植基於網路之上
- 網路摸不到、看不到，被攻擊了也不知道
- 能看到(Visualization)—流量監控
- 能分辨(Analysis)—流量分析
- 能判斷(Detection)—自動判斷攻擊行為
- 能阻擋(Prevention)—自動攔截惡意行為流量(SOAR)
- 能通報(Notification)—搭配SOC平台做到自動通報

應對

缺時間

善用資安聯防技術

TRUST: redefined



TRUST: redefined

Resources > Malware IPs > FortiGuard Malware IP

- Reports
- Rules
- Networks
- Watch Lists
- User Agents
- Remediations

New | Edit | Delete | More | Search...

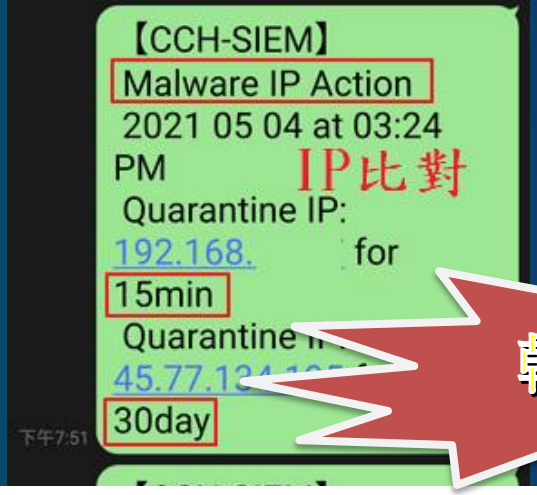
Last updated at Mar 9, 2021 5:02:56 PM

- Malware IPs
  - Emerging Threat Malware IP
  - Zeus Malware IP
  - ThreatStream Malware IP
  - FortiGuard Malware IP
  - TruSTAR Malware IP
  - ThreatConnect Malware IP
  - Ungrouped

1/7,217 | 360,577

Active	Low IP	Malware	Date Found
☑	1.0.132.173	Malware/F	
	1.0.135.102	Malware/F	
	1.0.135.188	Malware/F	
	1.0.135.206	Malware/F	
	1.0.135.28	Malware/F	
	1.0.135.48	Malware/F	
	1.0.135.8	Malware/F	
	1.0.137.149	Malware/PostInfectionTraffic	Spyware and Malware
	1.0.137.189	Malware/PostInfectionTraffic	Spyware and Malware
	1.0.164.92	Malware/PostInfectionTraffic	Spyware and Malware
	1.0.166.18	Malware/PostInfectionTraffic	Spyware and Malware
	1.0.166.49	Malware/PostInfectionTraffic	Spyware and Malware
	1.0.166.50	Malware/PostInfectionTraffic	Spyware and Malware
	1.0.166.63	Malware/PostInfectionTraffic	Spyware and Malware
	1.0.166.80	Malware/PostInfectionTraffic	Spyware and Malware
	1.0.215.194	Malware/PostInfectionTraffic	Spyware and Malware
	1.0.215.7	Malware/PostInfectionTraffic	Spyware and Malware
	1.0.217.113	Malware/PostInfectionTraffic	Spyware and Malware
	1.0.217.125	Malware/PostInfectionTraffic	Spyware and Malware
	1.0.217.127	Malware/PostInfectionTraffic	Spyware and Malware
	1.0.217.128	Malware/PostInfectionTraffic	Spyware and Malware
	1.0.218.19	Malware/PostInfectionTraffic	Spyware and Malware
☑	1.0.218.230	Malware/PostInfectionTraffic	Spyware and Malware
☑	1.0.219.117	Malware/PostInfectionTraffic	Spyware and Malware
☑	1.0.219.124	Malware/PostInfectionTraffic	Spyware and Malware

TRUST: redefined



韓劇小故事

您的裝置疑似中毒，有異

如需重新開通:

資訊設備 請聯絡資訊部

醫工設備 請聯絡醫工部

Log Details:

logver	60	idseq	1362391076
Time Stamp	2021-03-16 08:38:12	Device ID	FG5H1E5819
Device Name	FG	Virtual Domain	
Date	2021-03-16	Time	08:38:11
Log ID	0100	Type	event
Sub Type	system	Level	notice
eventtime	1615855091	Log Description	NAC quarantine
Source IP	10.10.40.183	Action	ban-ip
Banned Source	admin	admin	siem
Duration	900	Message	An administrative ban was created

Important Attacks

Top attacks, attack sources, and destinations.

Attack Types by Blades

76 IPS

1.5K Anti-Bot

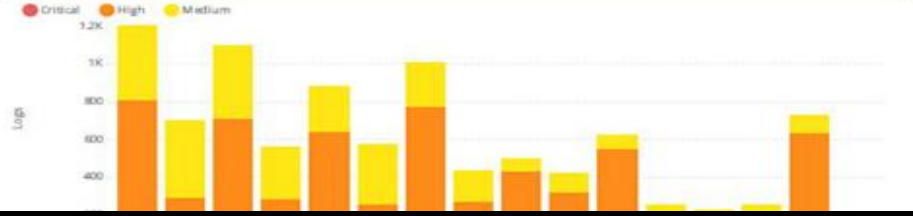
0 Threat Emulation

191 Anti-Virus

0 DDoS Protector

0 Threat Extraction

Activity Timeline



一定會被攻擊，不要期望完全防護，要學習跟攻擊共存

Dasan GPON Router Authentication Bypass	Critical	IPS	96
Dasan GPON Router Remote Command Injection	Critical	IPS	95
MVPower DVR Remote Code Execution	Critical	IPS	94
generic.TC.kzm	Critical	Anti-Virus	76
generic.TC.kvt	Critical	Anti-Virus	48
ZmEu Security Scanner	Critical	IPS	47
Generic.TC.hobfpz	Critical	Anti-Bot	40
Generic.TC.hktfqr	Critical	Anti-Bot	39
Generic.TC.ibbgai	Critical	Anti-Bot	36
Generic.TC.hhhesm	Critical	Anti-Bot	28
Total: 1722 Protections	**Critical**	**3 Blades**	**9.4K**

	Critical	Anti-Virus	24
	Critical	IPS	21
	Critical	Anti-Virus	20
	Critical	IPS	18
	Critical	IPS	17
	Critical	IPS	16
	Critical	IPS	14
	Critical	Anti-Virus	12
	Critical	Anti-Virus	11
Total: 1074 Sources	**Critical**	**3 Blades**	**9.4K**

	Critical	IPS	116
	Critical	Anti-Bot Anti-Virus IPS	113
	Critical	IPS	111
	Critical	Anti-Bot IPS	106
	Critical	Anti-Bot IPS	96
	Critical	Anti-Bot IPS	94
	Critical	IPS	88
Total: 232 Destinations	**Critical**	**3 Blades**	**9.4K**

應對

還是三缺

當資安人員不足，預算也不多

你可以規劃的計畫是...

老闆不想花錢，卻要求規劃資安，

你可以採購的資安產品是...

2021 資安大會
安全的奇點，與起點
奧義智慧科技 創辦人 邱銘彰 (Birdman)

EVERYTHING STARTS FROM CYCRAFT

奧義智慧 Proprietary and Confidential Information

TRUST: redefined

結語

IT Infras很辛苦

- 資訊網管人員 辛苦了!
- 資訊ISO人員 辛苦了!
- 網管+ISO，請多體諒他!
- 唐鳳：省力，安心，睡滿八小時
- 學會”健康的”舒壓

TRUST: redefined

Thank You