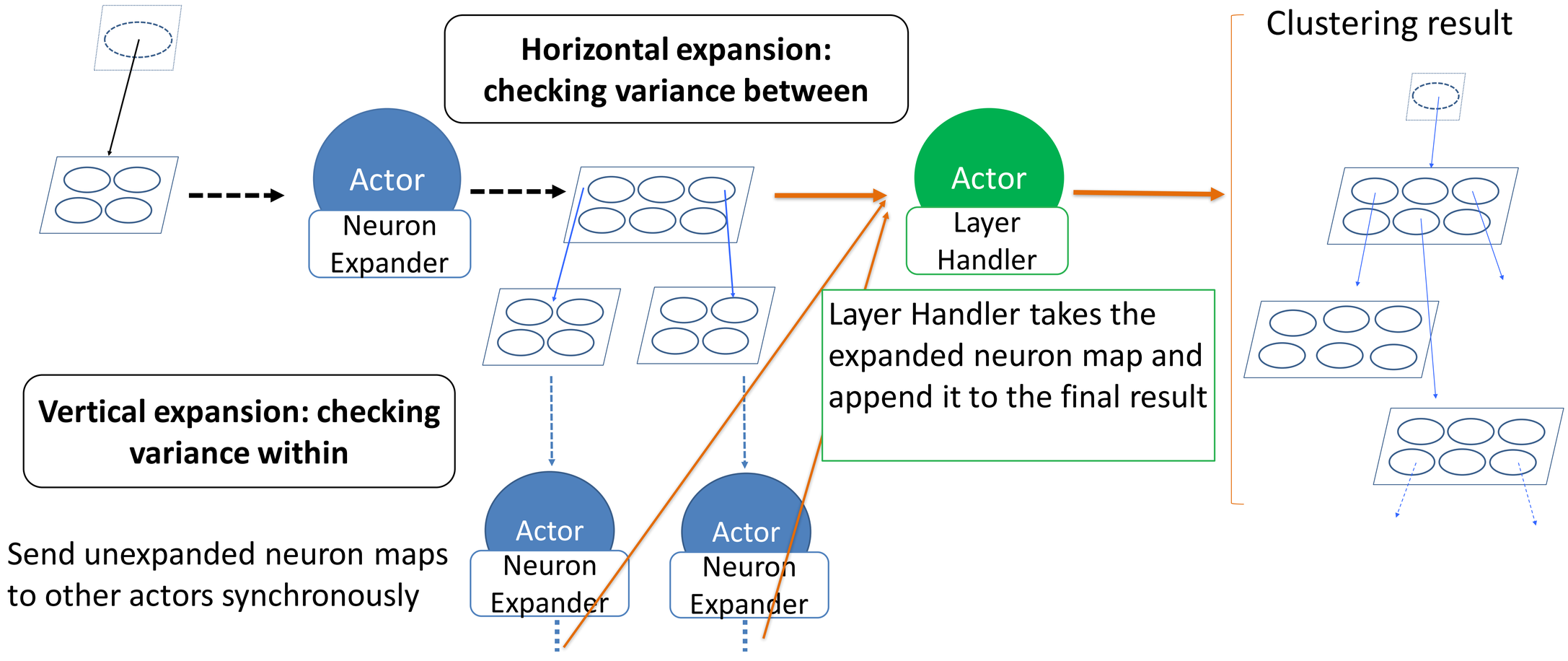
雲端服務之整體資安防禦系統
-開源碼雲端虛擬安全監測與人工智慧系統之研究
VISO: Unsupervised VM Behavior Clustering, Characterization and Detection

執行單位：國立政治大學資訊管理學系
主持人：郁方 副教授
計劃編號：103-2221-E-004 -006 -MY3

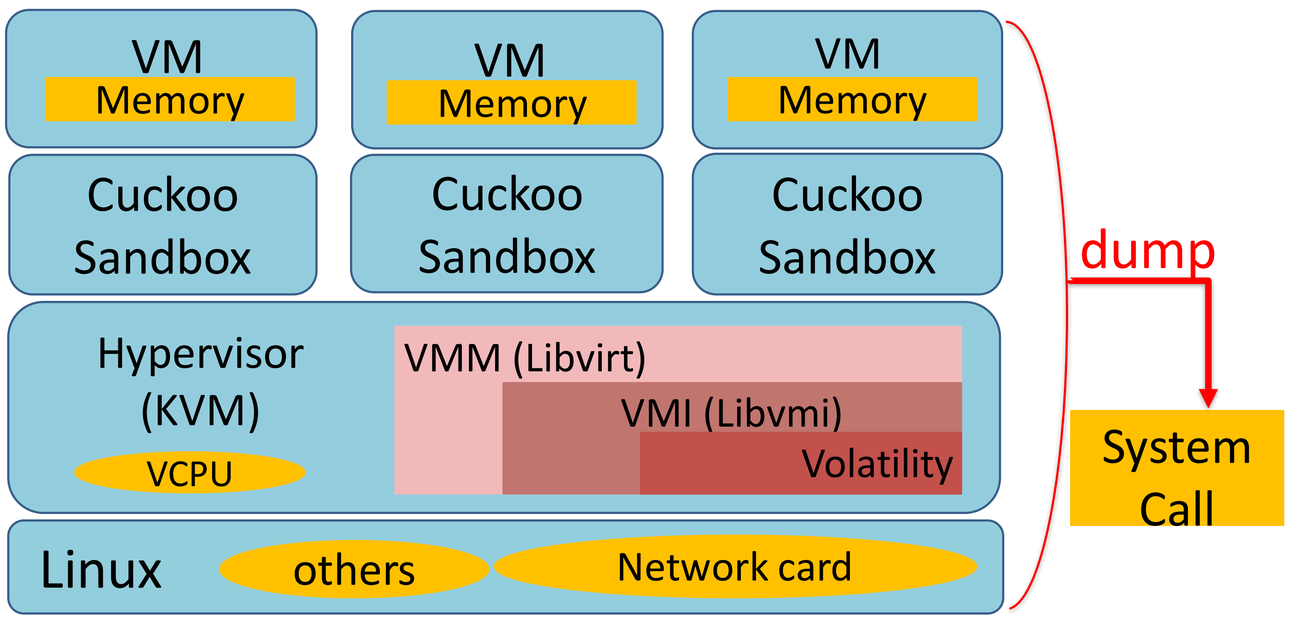
計畫摘要

本研究提出雲端虛擬安全監測與防禦系統(VISO)，期能補強開源碼的雲端平台安全性。其特點在於開發可規模化的非監督式分群技術，歸納監測虛擬系統的資訊與偵測規則。運用漸進式主體學習神經網路學習與彙整虛擬機惡意與異常行為的動態特徵, 進而形成防禦策略,偵測及預防虛擬機間的滲透與惡意的攻擊行為。

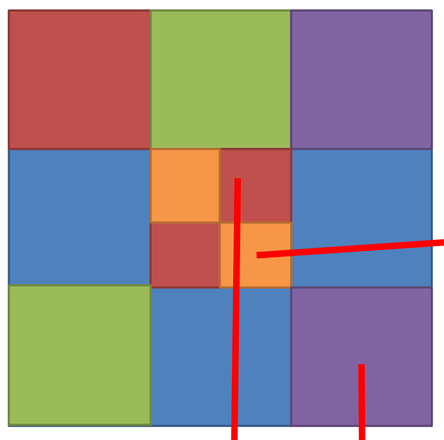
1.開發可規模化的非監督式分群演算模型



2.開發VISO實現線上VM系統呼叫側錄機制



3.依惡意行為分群訓練神經網路



Mal_ID_Period	Read	Write	Ioctl
Malware3_1	12	8	2
Malware3_2	13	7	1
Malware3_6	13	9	1

Mal_ID_Period	Read	Write	Ioctl
Malware1_1	5	3	8
Malware1_5	4	4	9

Mal_ID_Period	Read	Write	Ioctl
Malware1_4	8	9	10
Benign1_1	7	10	11

4.利用神經網路偵測線上VM惡意/異常行為

Rules	description
1	Win32/Allaple.155648、Win32/Sality.NAM、Win32/Conficker.X、Win32/Conficker.BL、Win32/Korgo.U、Win32/Conficker.AA、Win32/Korgo.V、Win32/Conficker.AE、Win32/Sality.NBE、Win32/Conficker.Gen、Win32/Flyagent.NGF
2	Win32/Conficker.X、Win32/Conficker.BL、Win32/Kryptik.AJRG、Win32/Neurevt.A、Win32/Pepex.E、Win32/Korgo.U、Win32/Conficker.AB、Win32/Conficker.AA、Win32/Korgo.V、Win32/AutoRun.AFQ、Win32/Conficker.AE、Win32/Confi
3	Win32/Allaple.Gen、Win32/Gobot.A、Win32/Allaple.155648、Win32/Neurevt.A、Win32/Pepex.E、Win32/Korgo.AA、Win32/Flyagent.NGF、Win32/Conficker.AS、Win32/Sasser.E、Win32/Kryptik.AJRG、Win32/Virut.AB、Win32/Conficker
4	Win32/Allaple.Gen、Win32/Gobot.A、Win32/Korgo.U、Win32/Korgo.AA、Win32/Flyagent.NGF、Win32/Sasser.E、Win32/Virut.AB、Win32/Conficker.AB、Win32/Conficker.AA、Win32/Conficker.AG、Win32/AutoRun.AFQ、Win32/Conficker
5	Win32/Allaple.Gen、Win32/Sality.NCR、Win32/Gobot.A、Win32/Agent.UOT、Win32/Korgo.U、Win32/Neurevt.A、Win32/Pepex.E、Win32/Korgo.AA、Win32/Flyagent.NGF、Win32/Conficker.AS、Win32/Sasser.E、Win32/Kryptik.AJRG、Win3
6	Win32/Allaple.Gen、Win32/Conficker.AE、Win32/Padobot.Z、Win32/Sality.NCR、Win32/Injector.IRT、Win32/Gobot.A、Win32/Kryptik.QEP、Win32/Allaple.A、Win32/TrojanDownloader.Agent、Win32/Agent.UOT、Win32/Allaple.1556
7	Win32/Allaple.Gen、Win32/Conficker.X、Win32/Conficker.BL、Win32/Allaple.A、Win32/Korgo.U、Win32/Conficker.AB、Win32/Conficker.AA、Win32/Korgo.V、Win32/Sality.NBE、Win32/Conficker.Gen
8	Win32/Conficker.AS、Win32/Allaple.Gen、Win32/Conficker.X、Win32/Sasser.E、Win32/Conficker.BL、Win32/Kryptik.AJRG、Win32/Neurevt.A、Win32/Conficker.Gen、Win32/Gobot.A、Win32/Korgo.U、Win32/Conficker.AB、Win32/Con
9	Win32/Allaple.Gen、Win32/Conficker.X、Win32/Conficker.BL、Win32/Sality.NCR、Win32/Korgo.U、Win32/Conficker.AB、Win32/Conficker.AA、Win32/Korgo.V、Win32/Conficker.AE、Win32/Sality.NBE、Win32/Conficker.Gen、Win32/
10	Win32/Conficker.X、Win32/Injector.FDW、Win32/Conficker.BL、Win32/Sality.NBE、Win32/Sasser.E、Win32/Korgo.U、Win32/Conficker.AB、Win32/Conficker.AA、Win32/Korgo.V、Win32/Conficker.AG、Win32/Conficker.AE、Win32/AI
11	Win32/Conficker.Z、Win32/Conficker.X、Win32/Injector.FDW、Win32/Conficker.BL、Win32/Kryptik.AJRG、Win32/Allaple.A、Win32/Pepex.E、Win32/Korgo.U、Win32/Conficker.AB、Win32/Conficker.AA、Win32/Korgo.V、Win32/Confi
12	Win32/Allaple.Gen、Win32/Conficker.AE、Win32/Sality.NCR、Win32/TrojanDownloader.Agent、Win32/Allaple.A、Win32/Agent.UOT、Win32/Pepex.I、Win32/Conficker.AS、Win32/Conficker.AB、Win32/Conficker.AA、Win32/AutoRun.
13	Win32/Allaple.Gen、Win32/Conficker.X、Win32/Conficker.BL、Win32/Pepex.E、Win32/Conficker.AB、Win32/Conficker.AA、Win32/Korgo.V、Win32/Conficker.AE、Win32/Conficker.Gen
14	Win32/Allaple.Gen、Win32/VB.QAZ、Win32/Padobot.Z、Win32/Sality.NCR、Win32/Injector.IRT、Win32/Virut.BF、Win32/Gobot.A、Win32/TrojanDownloader.Agent、Win32/Allaple.A、Win32/AutoRun.IRCBot、Win32/Injector.MAA、Win
15	Win32/Allaple.Gen、Win32/Conficker.X、Win32/Conficker.AA、Win32/Korgo.V、Win32/Korgo.AA、Win32/Conficker.Gen、Win32/Korgo.Z
16	Win32/Allaple.Gen、Win32/Conficker.X、Win32/Conficker.BL、Win32/Sality.NCR、Win32/Sality.NBE、Win32/Korgo.U、Win32/Conficker.AB、Win32/Conficker.AA、Win32/Korgo.V、Win32/Conficker.AE、Win32/Allaple.A、Win32/Conf
17	Win32/Allaple.Gen、Win32/Conficker.X、Win32/Injector.FDW、Win32/Conficker.BL、Win32/Sality.NCR、Win32/Sasser.E、Win32/Korgo.U、Win32/Conficker.AB、Win32/Conficker.AA、Win32/Korgo.V、Win32/Conficker.AE、Win32/Con
18	Win32/Injector.IXF、Win32/Allaple.Gen、Win32/Conficker.X、Win32/Sasser.E、Win32/Conficker.BL、Win32/Sality.NCR、Win32/Allaple.A、Win32/Korgo.U、Win32/Conficker.AA、Win32/Korgo.V、Win32/AutoRun.AFQ、Win32/Confick
19	Win32/Conficker.AS、Win32/Conficker.X、Win32/Conficker.BL、Win32/Sality.NCR、Win32/Allaple.A、Win32/Korgo.U、Win32/Conficker.AB、Win32/Conficker.AA、Win32/Korgo.V、Win32/Conficker.AE、Win32/Sality.NBE、Win32/Inj