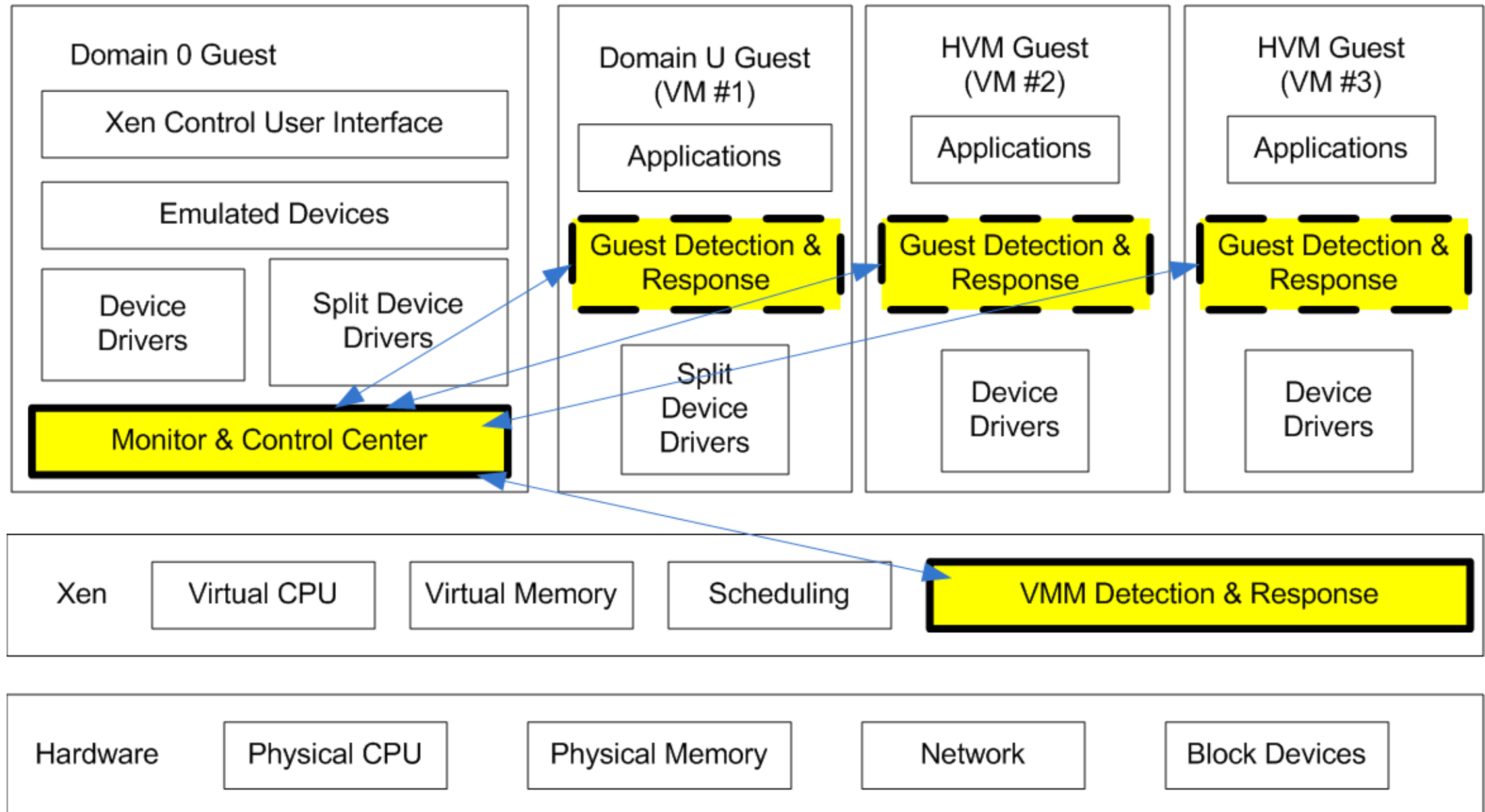
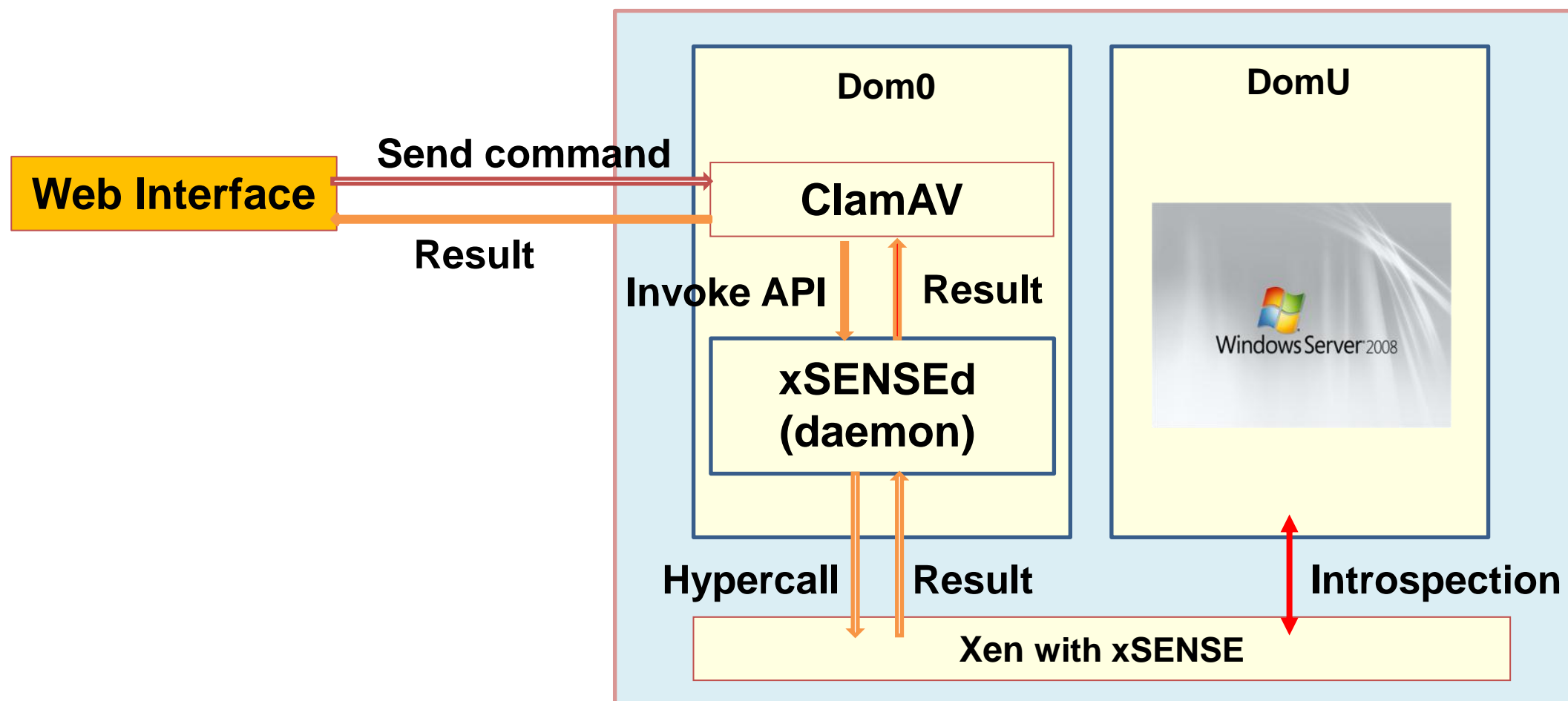


Hypervisor-based IDS/IPS 系統架構圖



Hypervisor-based IDS/IPS 應用實例：雲端防毒

- ClamAV：接受前端Web Interface的命令，透過定義好的 xSense API介面將命令傳給daemon，並將命令結果送回前端Web Interface顯示。
- Daemon：接受ClamAV的命令，透過Xen Hypercall介面將命令傳給Xen，並將命令結果傳回ClamAV。



成果可應用性-系統開發建置

Hypervisor-based 雲端防毒 - 系統運作畫面及流程

Laboratory of Security aNd SystEms | 安全系統實驗室

About Member Projects SenseVMs

Main Menu

[VM Portal]

Edit account info

Your team

Edit team info

Apply team vm

Manage team vm

Apply port for your vm

Publish team vm


[Logout]

Manage team virtual machine

Team vm

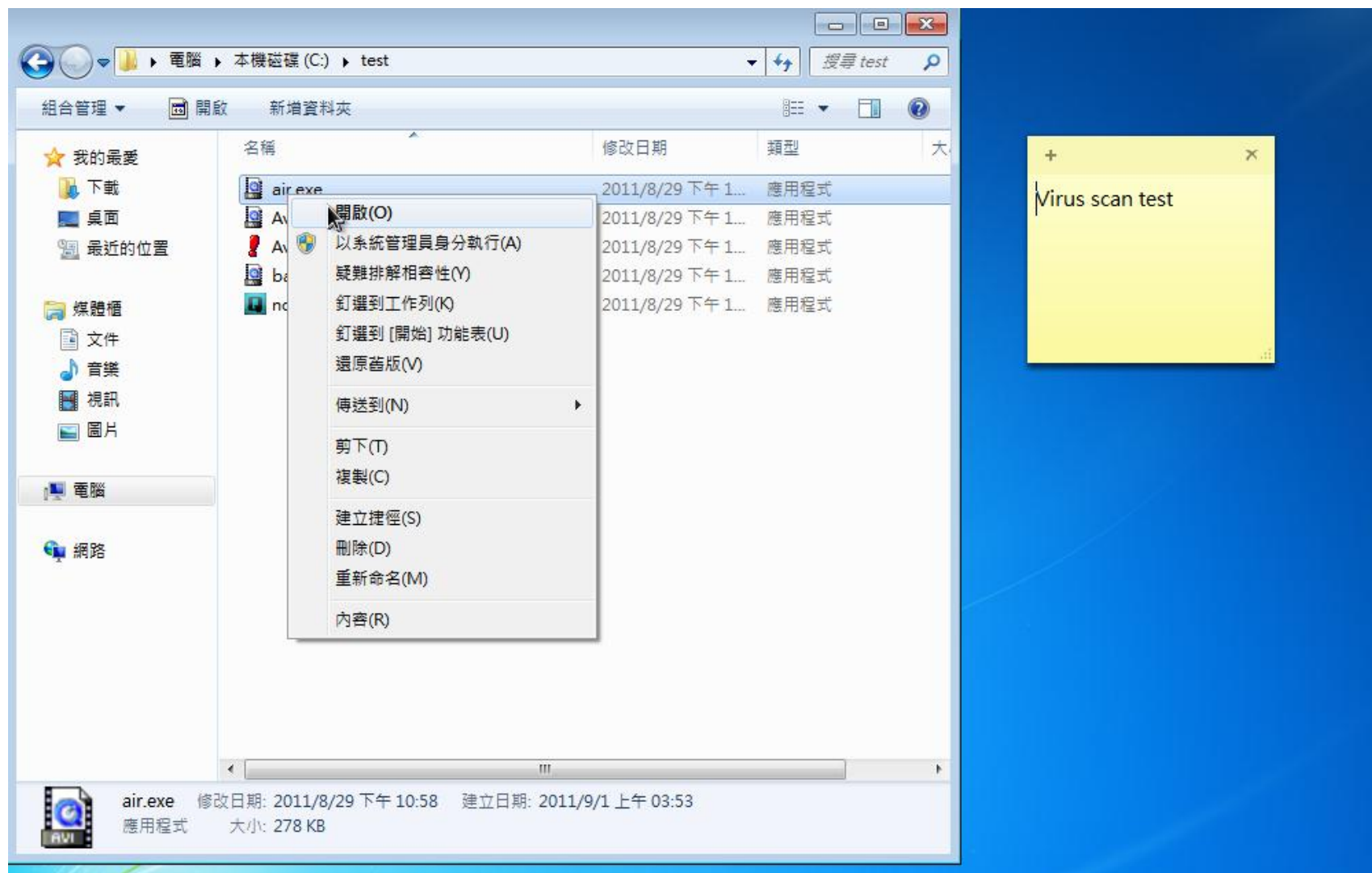
VM name	VM state	VM ip address	VNC address	Management	Continuation	Sleep Time	Delete	Antivirus
52_Win7_21113	running	192.168.20.11	140.113.88.181:21113	Force shutdown Sleep	Click	[16:48]	Delete	Antivirus

[VM Portal]



成果可應用性-系統開發建置

Hypervisor-based 雲端防毒 - 系統運作畫面及流程

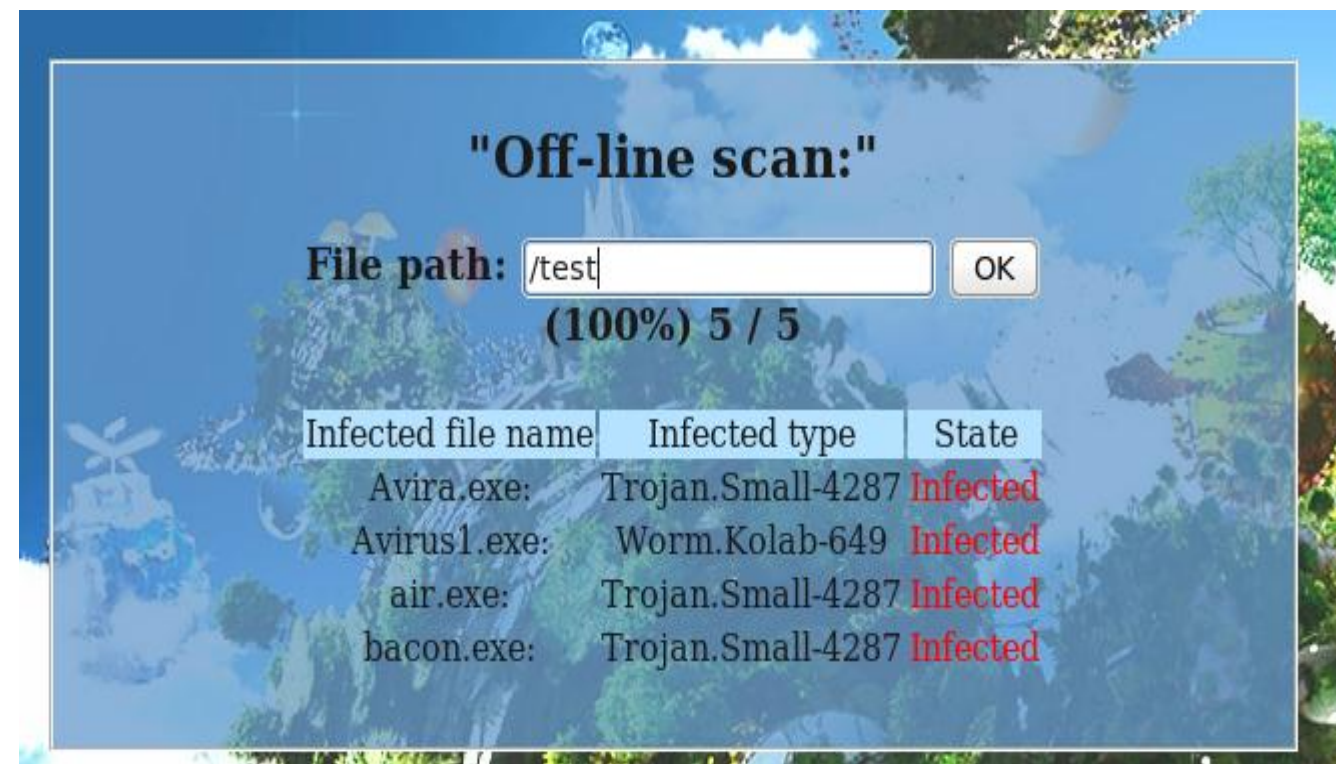


No need to install
anti-virus agents,
or any supporting
drivers in the VM

Accessing a virus-infected file in a Windows guest VM

成果可應用性-系統開發建置

Hypervisor-based 雲系統防毒 - 系統運作畫面及流程



雲系統防毒之Web控制介面 (Online Scan / Offline Scan)

成果可應用性-系統開發建置

Real-time monitoring of guest VM file access system call

```
(win num:2) path:\C:\test\air.exe count:403
PPPP:/test/air.exe
start copy-----
Get filehandle 0
filepath_temp:/home/temp_save_1/air.exe
count2:0
(win num:2) path:\C:\test\air.exe count:404
PPPP:/test/air.exe
start copy-----
Get filehandle 0
filepath_temp:/home/temp_save_1/air.exe
count2:0
(win num:2) path:\\C:\Windows\system32\twext.dll count:405
PPPP:/Windows/system32/twext.dll
(win num:2) path:\\C:\Windows\system32\twext.dll count:406
PPPP:/Windows/system32/twext.dll
(win num:2) path:\\C:\Windows\system32\twext.dll count:407
PPPP:/Windows/system32/twext.dll
(win num:2) path:H\C:\Windows\WinSxS\manifests\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.760
1.17514_none_fa396087175ac9ac.manifest count:408
(win num:2) path:H\C:\Windows\WinSxS\manifests\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.760
1.17514_none_fa396087175ac9ac.manifest count:409
(win num:2) path:H\C:\Windows\WinSxS\manifests\amd64_microsoft.windows.c...-controls.resources_6595b64144ccf1df_
6.0.7600.16385_zh-tw_73f243ac283c6b65.manifest count:410
(win num:2) path:H\C:\Windows\WinSxS\manifests\amd64_microsoft.windows.c...-controls.resources_6595b64144ccf1df_
6.0.7600.16385_zh-tw_73f243ac283c6b65.manifest count:411
(win num:2) path:\C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_non
e_fa396087175ac9ac count:412
(win num:2) path:\C:\Windows\system32\zh-TW\twext.dll.mui count:413
PPPP:/Windows/system32/zh-TW/twext.dll.mui
(win num:2) path:\C:\ count:414
PPPP:/
(win num:2) path:\C:\Users\desktop.ini count:415
PPPP:/Users/desktop.ini
```

ClamAV reads the file for scanning via xSense API

Dom0 daemon (xSensed)

SENSE Lab



■ 技術方案優越性

- 集中監測所有虛擬機，虛擬機本身不須安裝入侵偵測系統，節省各自維護的時間與人力成本。
- 隱匿入侵偵測系統，惡意程式將無法得知自己身在監測環境之中。
- 提高入侵偵測系統層級權限，惡意程式將無法攔截或竄改入侵偵測系統所執行的命令。

