SecuTex

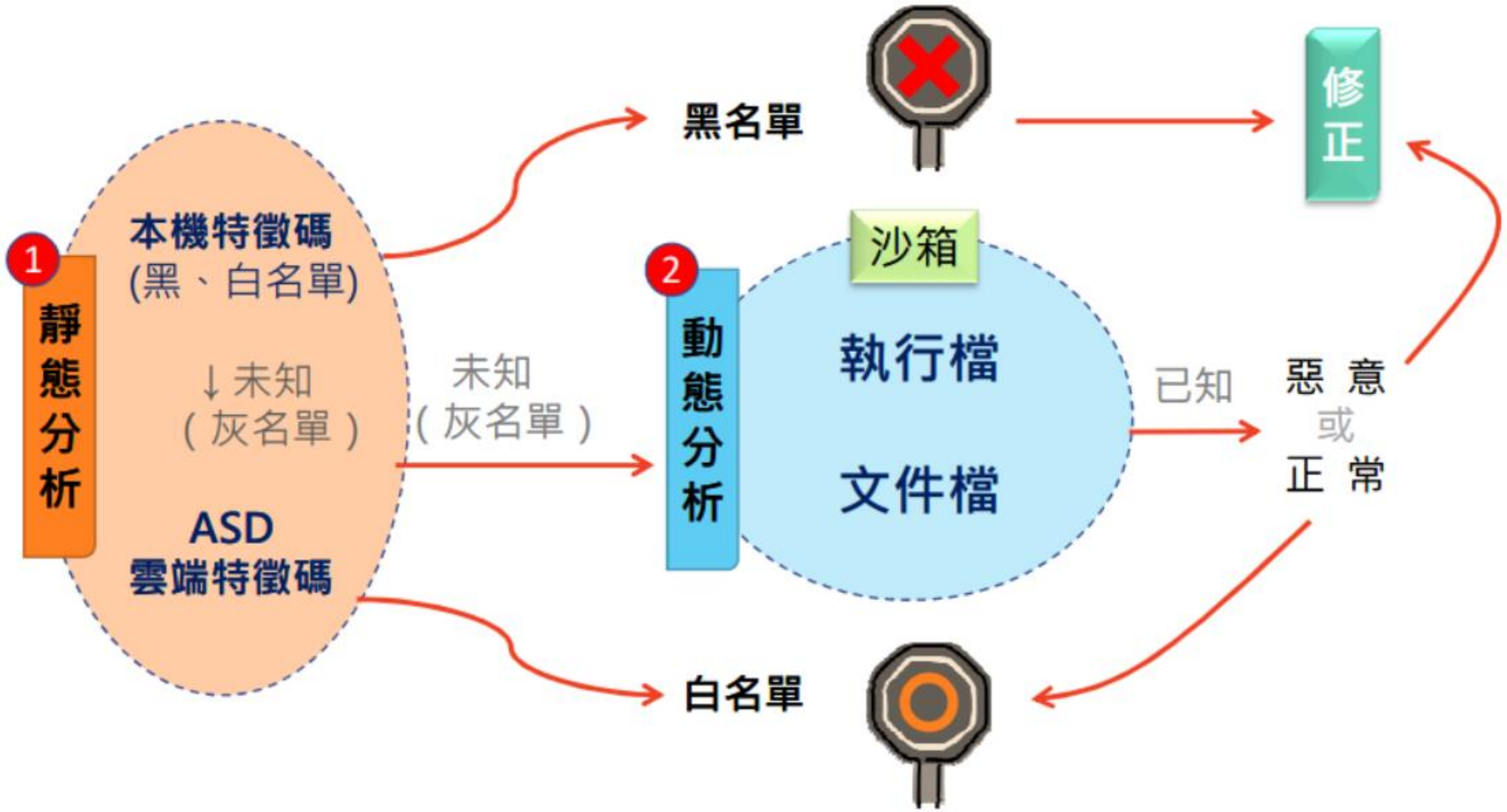
SecuTeX 惡意檔案威脅分析系統

APT 解決方案

網路瀏覽偵測

惡意檔案與郵件偵測

偵測機制


1
靜態分析
本機特徵碼
(黑、白名單)
↓未知
(灰名單)
ASD
雲端特徵碼
黑名單
白名單
未知
(灰名單)
2
動態分析
沙箱
執行檔
文件檔
已知
惡意
或
正常
修正

沙箱分析引擎與技術

A. **Memory analysis** : 分析漏洞被觸發後可能產生的Heap Spray（堆 / 棧溢出，目的為執行特定之惡意指令shellcode）。

B. **Assembly level analysis** : 透過反組譯分析。

C. **Shellcode analysis** : 分析惡意指令（shellcode）所在位置。

即便該惡意程式並未在沙箱內觸發惡意行為，亦可有效偵測，可彌補傳統沙箱僅依據行為分析結果來判斷惡意程式之不足，因為新型態的惡意程式通常也具備規避沙箱的能力。

補充: 分析檔案類型

PE檔：

AX, BIN, COM, DLL, EXE, MTX, OCX, PRC, SCR, SYS, VXD

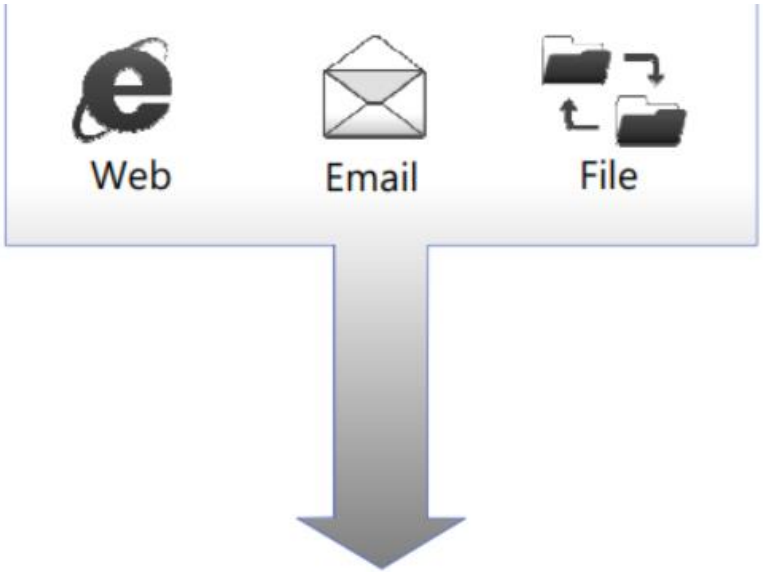
Non-PE檔：

doc(x), ppt(x), xls(x), pdf, hwp, SHS, ASP, BAS, BAT, CHM, DRV, EML, HTA, HTM, HTML, HTT, INI, JS, JSE, KEY, LNK, MRC, NWS, PHP, PIF, PL, SH, VBE, VBS, DIET, LZEXE, PKLITE, gif, bmp, pdf, jpeg, jpg, jpe, png

 # 除預設檔案類型外，亦可自行定義新增File extension。

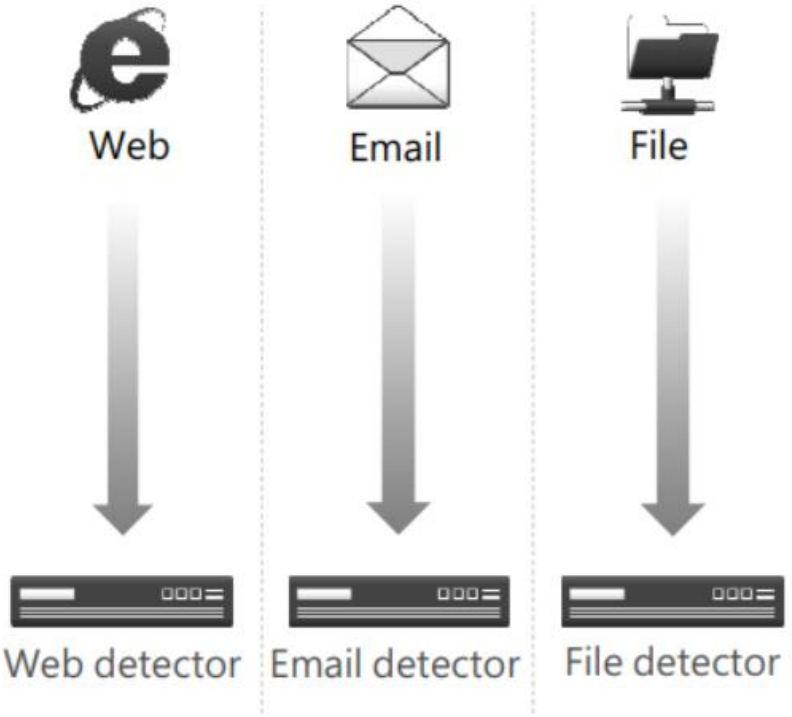
Protocol	PE Files	Non-PE Files				
		Document	Macro	Script	Compressed Executable	Image
HTTP, FTP, SMB, POP3, IMAP, SMTP, NFS	AX, BIN, COM, DLL, EXE, MTX, OCX, PRC, SCR, SYS, VXD	doc(x), ppt(x), xls(x), pdf, hwp	Doc(x), xls(x), ppt(x), SHS	ASP, BAS, BAT, CHM, DRV, EML, HTA, HTM, HTML, HTT, INI, JS, JSE, KEY, ..LNK, MRC, NWS, PHP, PIF, PL, SH, VBE, VBS	DIET, LZEXE, PKLITE	gif, bmp, pdf, jpeg, jpg, jpe, png

高成本效益，一台搞定！



SecuTex 沙相

VS



流量擷取，佈建容易

支援MTA