系統也要定期健檢
由系統內部進行入侵偵測與合規性檢測
HIDS & Compliance

主講者:Stev

主講者簡介

任職於臺灣證券交易所，負責交易系統安全維運、系統合規作業。

專長領域包括系統安全強化、網路安全、日誌監控、資訊合規稽核、IoT、工業控制協定及SCADA系統，擅長整合資訊技術及應用。

曾獲選台北市政府技能優異勞工，取得國際認證：CISSP、CEH、CCSK、RHCE、CISA、ISO20000LA、ISO27001LA。

議程大綱

1. 入侵偵測系統簡介
2. 整合式入侵偵測系統介紹
   - OSSEC入侵偵測系統工具
3. 系統合規性檢測
   - SCAP協定介紹
   - OpenSCAP合規性檢測工具-for Linux
   - LGPO合規性檢測工具-for Window
4. 以弱點掃瞄工具驗證系統安全性
5. 結論

入侵偵測系統 Intrusion Detection System

透過比對「主機行為」、「安全日誌」、「稽核軌跡」或「入侵特徵資訊」，進行研判與比對，檢測出入侵企圖或疑似系統被入侵的異常行為，比對行為又可分為「特徵比對」和「異常比對」。進行入侵偵測的軟體、硬體組合便是入侵偵測系統。

入侵偵測系統原理

Signature-Based 特徵偵測

透過偵測攻擊特徵(patterns) 尋找被入侵的跡象，例如檔案位元異動、異常網路流量或已知的惡意攻擊特徵。這個偵測方式源自防毒軟體，可輕易偵測已知的攻擊。

缺點：

- 無法偵測新型態入侵，因無特徵值比對(False Negative)。
- 特徵相符也可能非入侵行為造成假警報(False Positive)。
- 必須進行大量特徵比對，可能造成系統負荷過重。

入侵偵測系統原理

Anomaly-Based 異常偵測

由於惡意軟體更新的速率越來越快速，異常偵測主要用來偵測未知的攻擊。通常會建立正常行為的標準值，當超過門檻時會觸發告警，通常採正面表列，即不在正常範圍內的行為均視為異常。

缺點：

- 系統穩定需要較長的磨合期
- 合法行為可能會被誤判造成假警報(False Postive)

入侵偵測系統種類

Network-based Intrusion Detection System 網路式入侵偵測系統

對網路骨幹側錄的網路封包進行特徵比對，確認有無入侵行為，屬事前預警誤報率較高，佈署較為容易但無法即時偵測加密傳輸內容。

Host-based Intrusion Detection System 主機式入侵偵測系統

安裝於主機內可監看系統檔案、屬性有無未經授權變更，屬事後分析誤報率較低，佈署更新較麻煩資源需要也較高。安全性依賴於主機端作業系統。

免費軟體--入侵偵測系統比較矩陣

HIDS NIDS

Free software [edit]

As per the Unix philosophy a good HIDS is composed of multiple packages each focusing on a specific aspect.

Package	Year[1]	Ubuntu[2]	CentOS[3]	File	Network	Logs	Config	Sane defaults	Notes
OSSEC	2017	No	No	Yes	Yes	Yes	Yes		
Lynis	2017	Partial[4] broken	Yes[5]	No	No	No	Yes	Yes	Compliance testing only in the commercial version
OpenVAS	2017	No	No	No	No	No	Yes		
Samhain	2016	Yes[6]	No	Yes	No	Partial[7]		No	
Snort	2015	Yes[8]	No	No	Yes	No			
chkrootkit	2017	Yes[9]	No	Yes	No	Partial[10]			
rkhunter	2014	Yes[11]	Yes[12]	Yes	No	No	Yes	Yes	
unhide[13]	2012	Yes[14]	Yes[15]	No	No	No			proc ps compare
Sguil	2017	No	No	No	Yes	No			
Logwatch[16]	2017	Yes[17]	Yes[18]	No	No	Yes		No	
Logcheck[19]	2017	Yes[20]	Yes[21]	No	No	Yes		No	
Epylog[22]	2014	Yes[23]	Yes[24]	No	No	Yes			
SWATCH[25]	2015	Yes[26]	Yes[27]	No	No	Yes			
sagan	2017	Yes[28]	No	No	No	Yes			
aide	2016	Yes[29]	Yes[30]	Yes	No	No		No	
tripwire	2013	Yes[31]	Yes[32]	Yes	No	No			

資料來源 https://en.wikipedia.org/

整合式入侵偵測系統架構

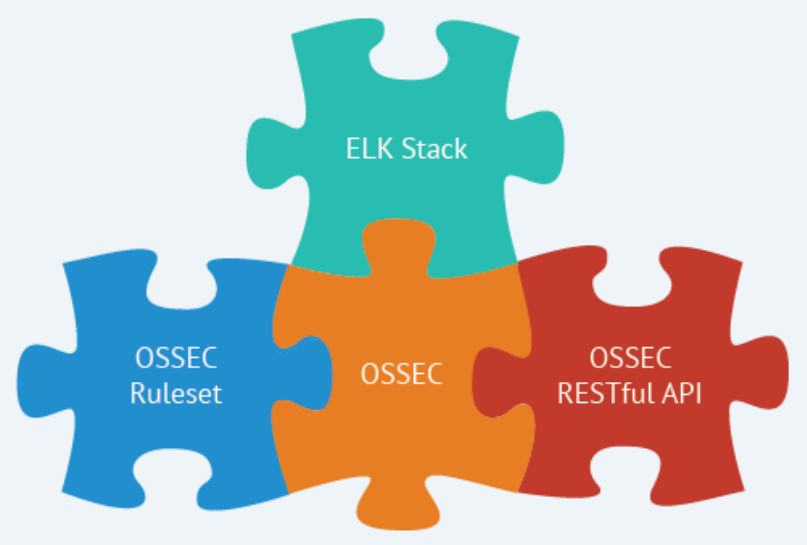
整合式入侵偵測系統架構

Wazuh - Open Source Host and Endpoint Security

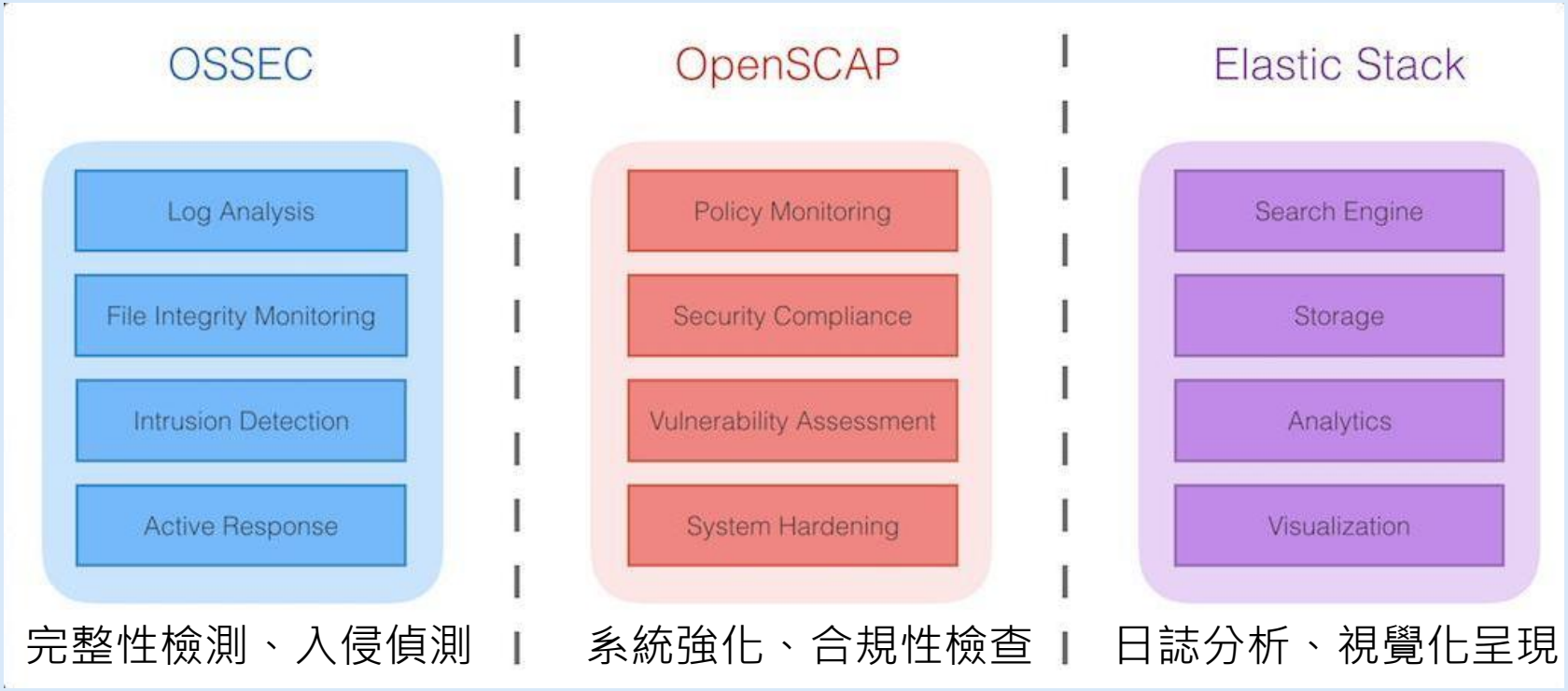
OSSEC + ELK + OpenSCAP regulation ruleset

https://documentation.wazuh.com/

https://wazuh.com/pci-dss/



整合式入侵偵測系統架構



完整性檢測、入侵偵測 | 系統強化、合規性檢查 | 日誌分析、視覺化呈現

稽核報表產出

圖片來源 Wazuh.com
文件詳見 https://documentation.wazuh.com

OSSEC入侵偵測系統工具重要功能

Log Monitoring	→	監控各種日誌檔案，協助重要訊息監看
File Integrity checking	→	檢查檔案屬性，發現未經授權的變更
Intrusion detection	→	偵測潛伏於系統的惡意軟體/後門程式
Active response	→	發現異常事件後主動執行相關防護措施 避免影響擴散

OSSEC入侵偵測系統優點分析

Compliance Requirements → PCI DSS/USGCB

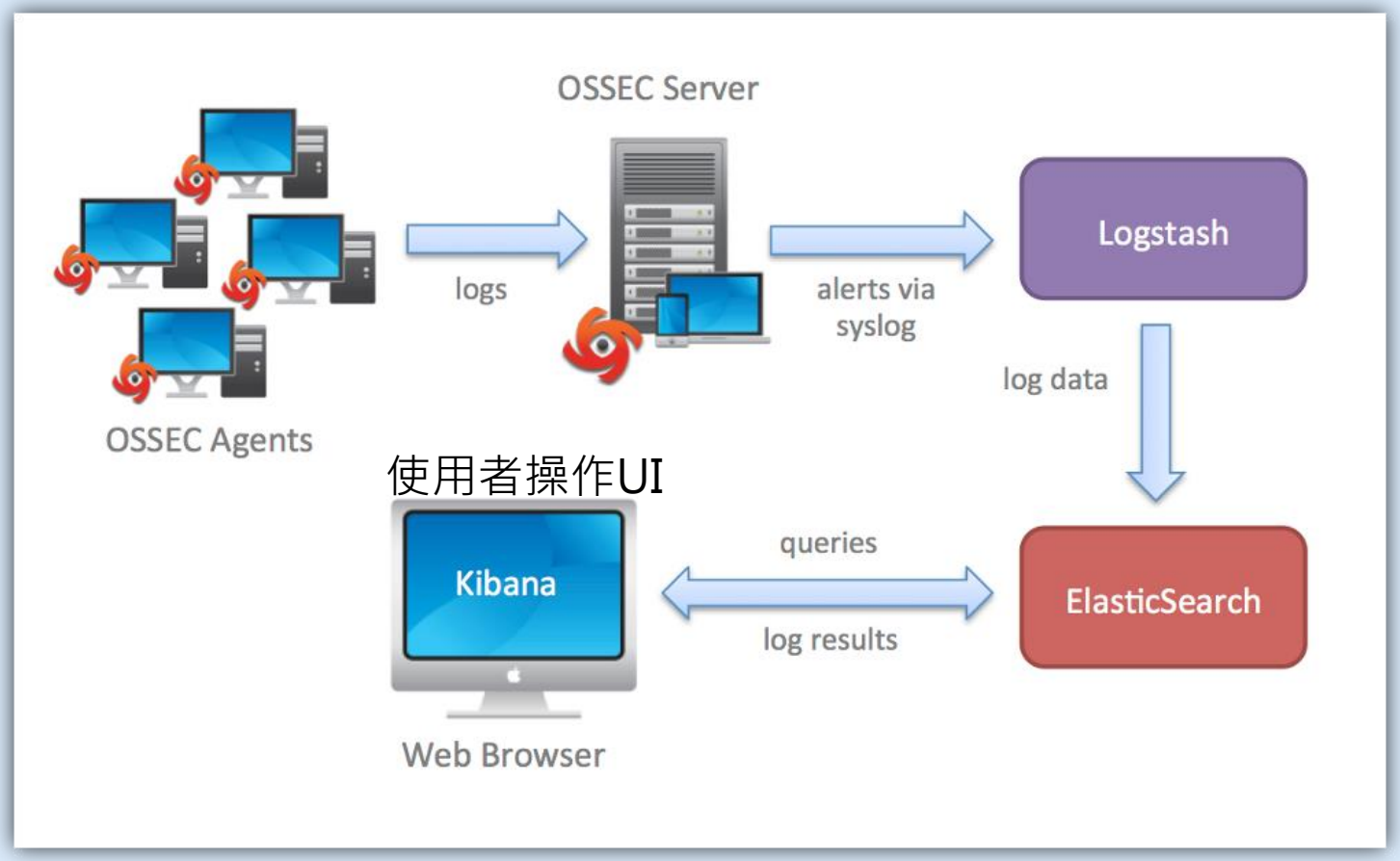
Support multi platform → Linux, Solaris, Windows, Mac OS X

Real-time and Configurable Alerts → smtp, syslog, json

Support agentless monitoring → Firewalls, switches and routers

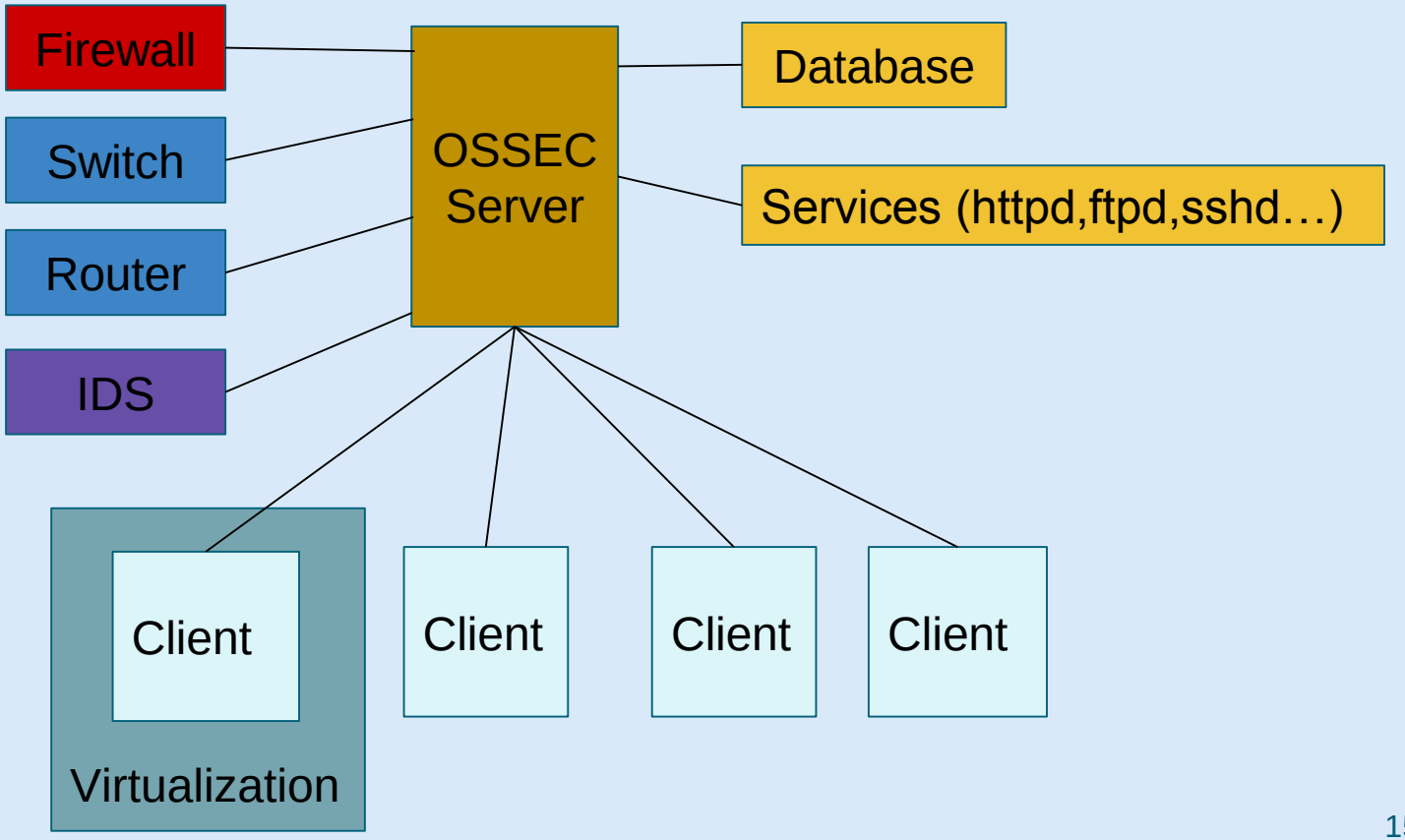
Integration with current infrastructure
Centralized management

OSSEC+Elastic Stack 系統架構



圖片來源 vichargrave.github.io

OSSEC入侵偵測系統可收容監看設備



OSSEC入侵偵測系統軟體架構

Local/Server/Agent 三種模式

OSSEC Agent

Agentd：Forwards data to the server

Logcollectord：Read logs (log,wmi,flatfiles)

Syscheckd　　：File integrity checking

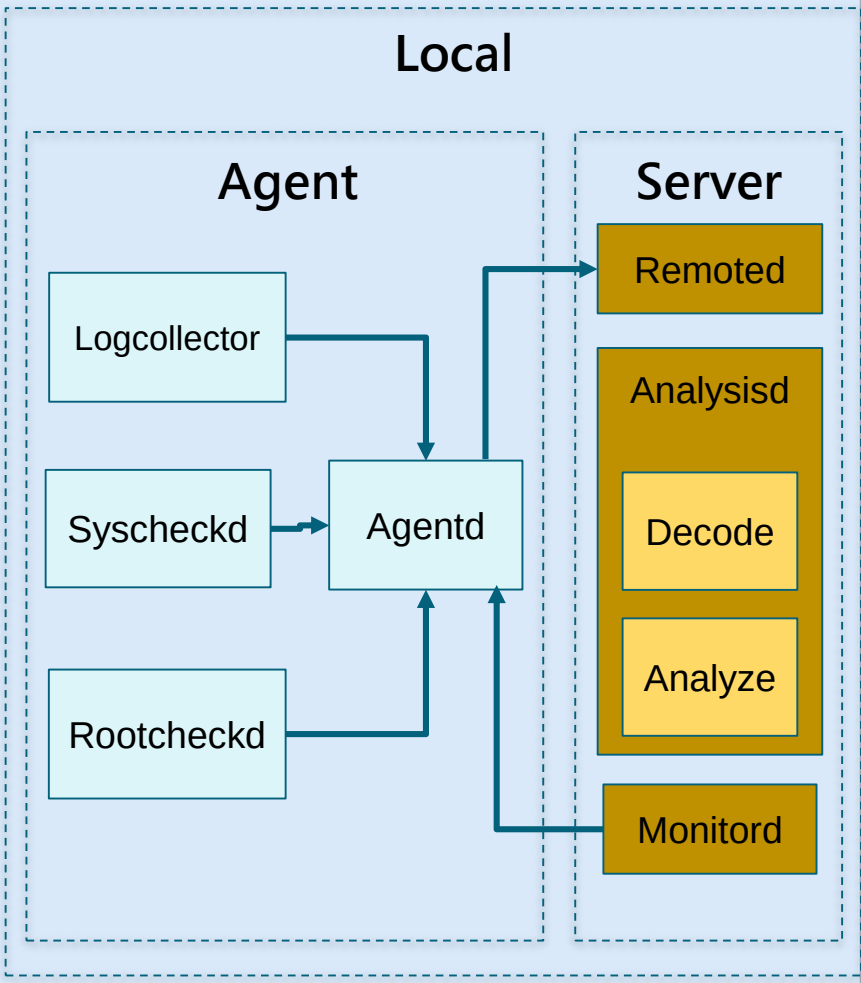
Rootcheckd：Malware and rootkits detection

OSSEC Server

Remoted：Receives data from agents

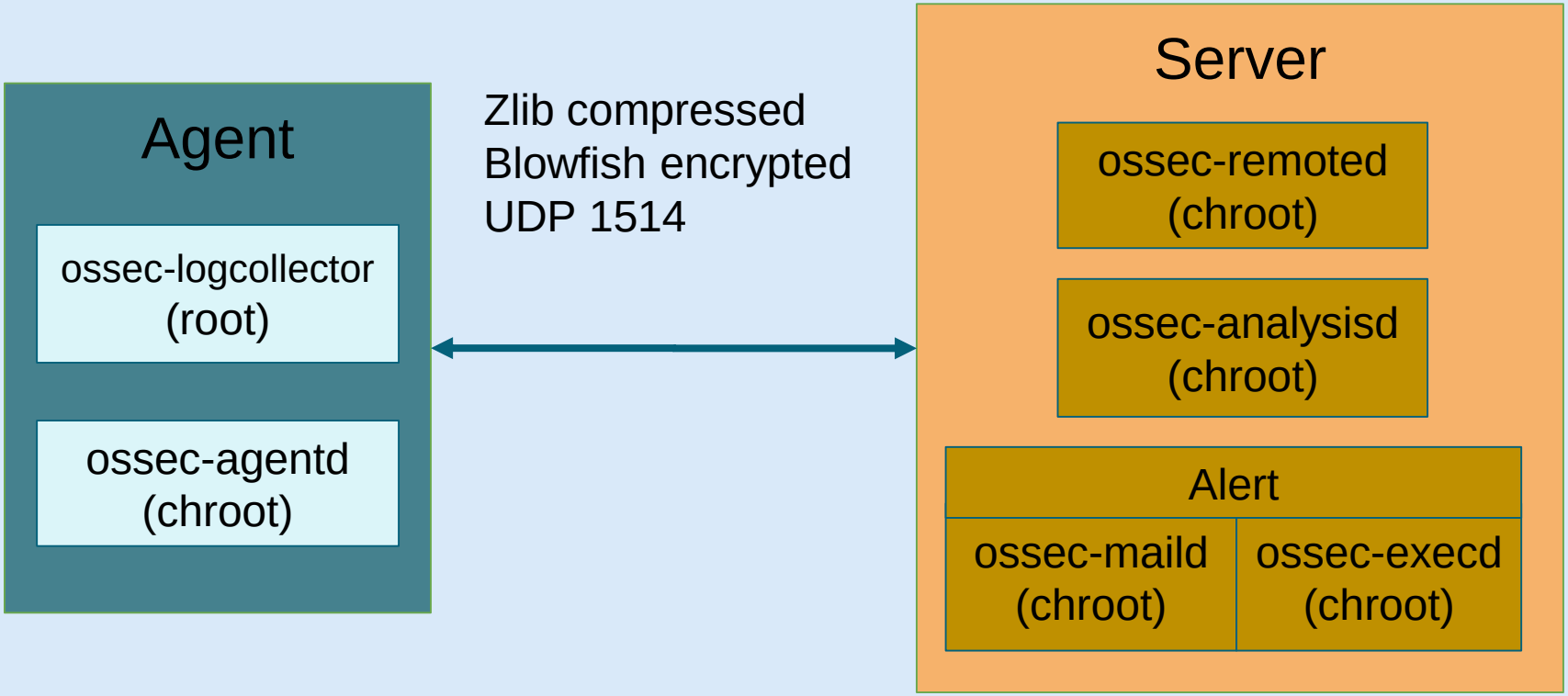
Analysisd：Processes data (main process)

Monitord：Monitor agents

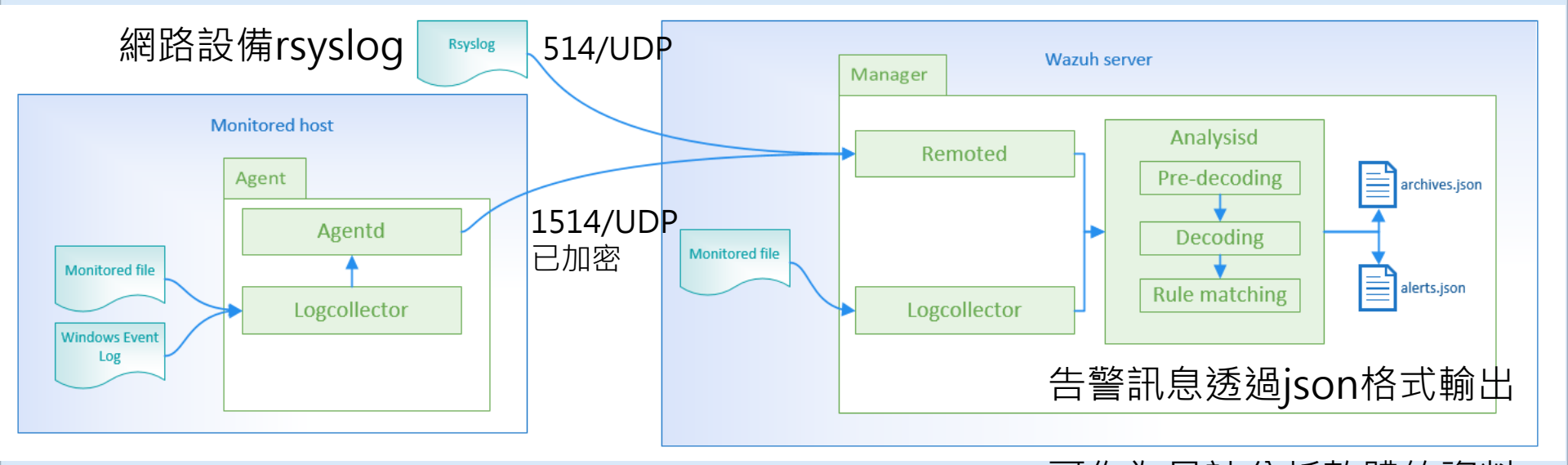


OSSEC入侵偵測系統軟體架構

主從架構通訊方式經過壓縮後加密，透過UDP傳輸



Log monitoring flow 系統日誌監控資料流



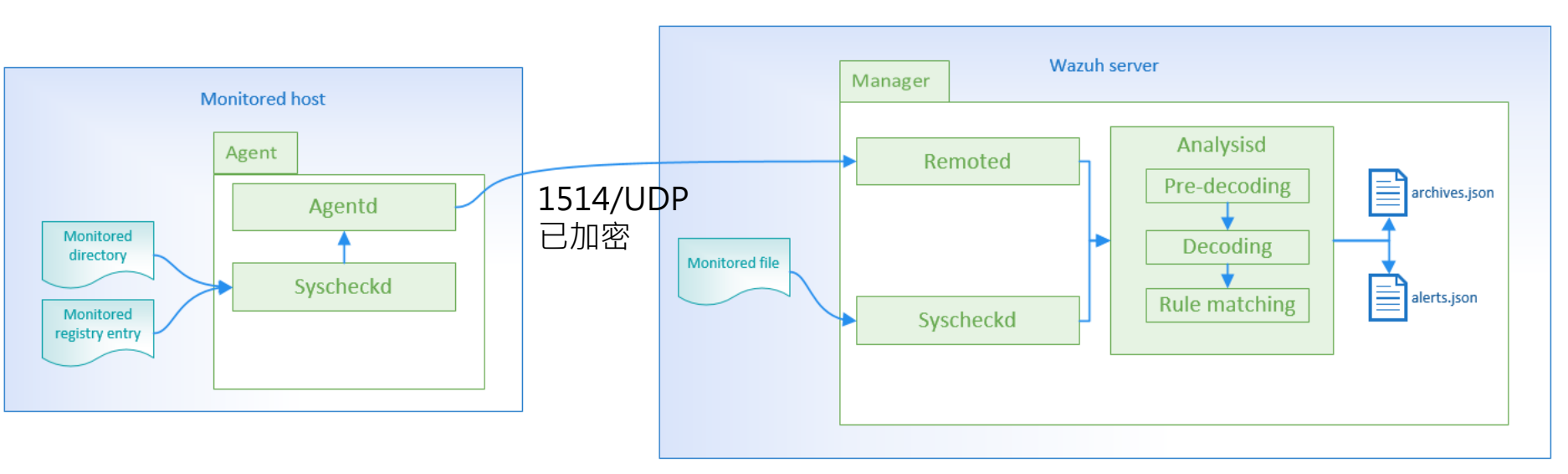
可作為日誌分析軟體的資料來源(source data)

支援安裝agent的系統：
Linux, Windows, Mac OS X, Solaris

圖片來源 Wazuh.com
文件詳見 https://documentation.wazuh.com

File integrity monitoring flow檔案完整性資料流

不支援agentless (網路設備)

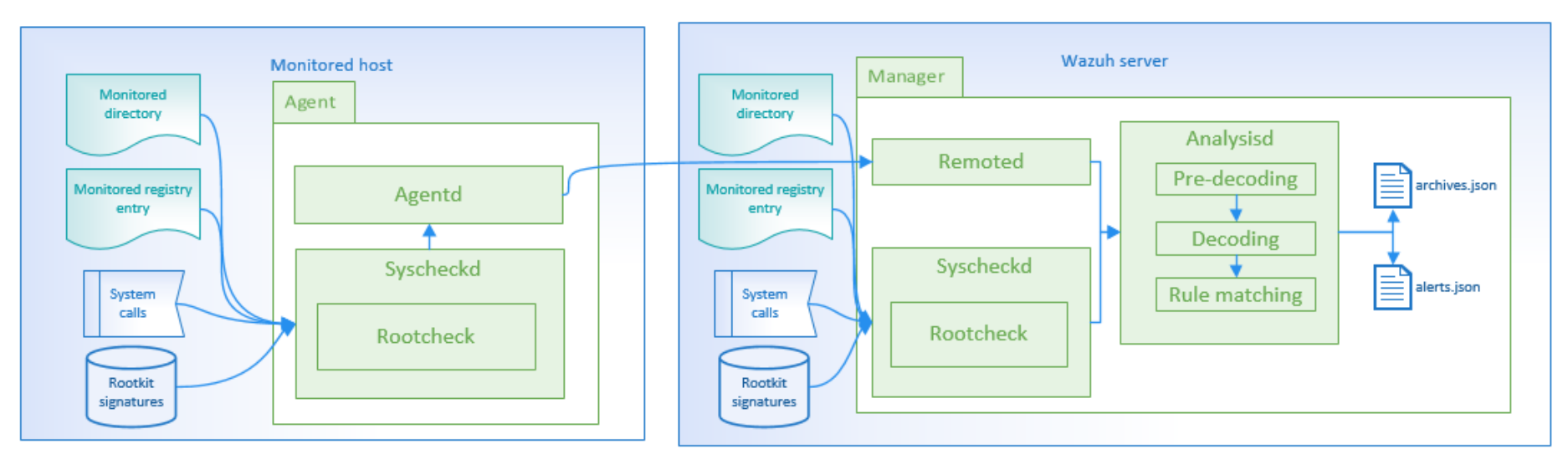


支援安裝agent的系統：
Linux, Windows, Mac OS X, Solaris

圖片來源 Wazuh.com
文件詳見 https://documentation.wazuh.com

Rootkit detection flow後門工具檢測資料流

不支援agentless (網路設備)



Rootkit特徵資料庫

圖片來源 Wazuh.com
文件詳見 https://documentation.wazuh.com

OSSEC預設系統檔案目錄

預設安裝目錄 /var/ossec/

主要設定檔目錄 /var/ossec/etc/

命令執行檔目錄 /var/ossec/bin/

告警規則 /var/ossec/ruleset/rules/*.xml

告警規則以XML形式儲存
Rules are hierarchical
Already include rules for :
apache, cisco-ios, firewalls, ftp …
and more

解碼規則以XML形式儲存
Extracts data from log entries to alert matching including:
IP/Port/Process name and more

Decoders解碼器 /var/ossec/ruleset/decoders/*.xml

系統日誌目錄 /var/ossec/logs/

告警日誌目錄 /var/ossec/logs/alerts/

OSSEC環境介紹

重要設定檔/var/ossec/etc/

ossec.conf OSSEC主要設定檔

internal_options.conf OSSEC相關daemon參數

重要系統安全性檢查 /var/ossec/etc/shared/

cis_xxx_linux_rcl.txt 各版本Linux安全性檢查清單

rootkit_files.txt 蠕蟲與惡意檔案檢查清單

rootkit_trojans.txt 木馬程式檢查清單

OSSEC環境介紹

預設日誌解碼規則 /var/ossec/ruleset/decoders

針對不同的系統服務有相對應的xml檔案日誌解碼格式

```
[root@wazuh-server decoders]# ls
0010-active-response_decoders.xml  0110-ftpd_decoders.xml          0210-pix_decoders.xml                0310-ssh_decoders.xml
0015-aix-ipsec_decoders.xml        0115-grandstream_decoders.xml   0215-portsentry_decoders.xml         0315-su_decoders.xml
0020-amazon_decoders.xml           0120-horde_decoders.xml         0220-postfix_decoders.xml            0320-sudo_decoders.xml
0025-apache_decoders.xml           0125-hp_decoders.xml            0225-postgresql_decoders.xml         0325-suhosin_decoders.xml
0030-arpwatch_decoders.xml         0130-imapd_decoders.xml         0230-proftpd_decoders.xml            0330-symantec_decoders.xml
0035-asterisk_decoders.xml         0135-imperva_decoders.xml       0235-puppet_decoders.xml             0335-telnet_decoders.xml
0040-auditd_decoders.xml           0140-kernel_decoders.xml        0240-pure-ftpd_decoders.xml          0340-trend-osce_decoders.xml
0045-barracuda_decoders.xml        0145-mailscanner_decoders.xml   0245-racoon_decoders.xml             0345-unbound_decoders.xml
0050-checkpoint_decoders.xml       0150-mysql_decoders.xml         0250-redis_decoders.xml              0350-unix_decoders.xml
0055-cimserver_decoders.xml        0155-named_decoders.xml         0255-roundcube_decoders.xml          0355-vm-pop3_decoders.xml
0060-cisco-estreamer_decoders.xml  0160-netscaler_decoders.xml     0260-rsa-auth-manager_decoders.xml   0360-vmware_decoders.xml
0065-cisco-ios_decoders.xml        0165-netscreen_decoders.xml     0265-rshd_decoders.xml               0365-vpopmail_decoders.xml
0070-cisco-vpn_decoders.xml        0170-nginx_decoders.xml         0270-samba_decoders.xml              0370-vsftpd_decoders.xml
0075-clamav_decoders.xml           0175-ntpd_decoders.xml          0275-sendmail_decoders.xml           0375-web-accesslog_decoders.xml
0080-courier_decoders.xml          0180-openbsd_decoders.xml       0280-serv-u_decoders.xml             0380-windows_decoders.xml
0085-dovecot_decoders.xml          0185-openldap_decoders.xml      0285-snort_decoders.xml              0385-wordpress_decoders.xml
0090-dragon-nids_decoders.xml      0190-openvpn_decoders.xml       0290-solaris_decoders.xml            0390-zeus_decoders.xml
0095-dropbear_decoders.xml         0195-oscap_decoders.xml         0295-sonicwall_decoders.xml
```

OSSEC環境介紹

預設服務檢查規則 /var/ossec/ruleset/rules

針對不同的系統服務有相對應的xml檔案描述監控事件

```
[root@wazuh-server rules]# ls
0010-rules_config.xml        0115-arpwatch_rules.xml          0220-msauth_rules.xml       0325-opensmtpd_rules.xml
0015-ossec_rules.xml         0120-symantec-av_rules.xml       0225-mcafee_av_rules.xml    0330-sysmon_rules.xml
0020-syslog_rules.xml        0125-symantec-ws_rules.xml       0230-ms-se_rules.xml        0335-unbound_rules.xml
0025-sendmail_rules.xml      0130-trend-osce_rules.xml        0235-vmware_rules.xml       0340-puppet_rules.xml
0030-postfix_rules.xml       0135-hordeimp_rules.xml          0240-ids_rules.xml          0345-netscaler_rules.xml
0035-spamd_rules.xml         0140-roundcube_rules.xml         0245-web_rules.xml          0350-amazon_rules.xml
0040-imapd_rules.xml         0145-wordpress_rules.xml         0250-apache_rules.xml       0355-amazon-ec2_rules.xml
0045-mailscanner_rules.xml   0150-cimserver_rules.xml         0255-zeus_rules.xml         0360-serv-u_rules.xml
0050-ms-exchange_rules.xml   0155-dovecot_rules.xml          0260-nginx_rules.xml        0365-auditd_rules.xml
0055-courier_rules.xml       0160-vmpop3d_rules.xml           0265-php_rules.xml          0370-amazon-iam_rules.xml
0060-firewall_rules.xml      0165-vpopmail_rules.xml          0270-web_appsec_rules.xml   0375-usb_rules.xml
0065-pix_rules.xml           0170-ftpd_rules.xml              0275-squid_rules.xml        0380-redis_rules.xml
0070-netscreenfw_rules.xml   0175-proftpd_rules.xml          0280-attack_rules.xml       0385-oscap_rules.xml
0075-cisco-ios_rules.xml     0180-pure-ftpd_rules.xml         0285-systemd_rules.xml      0390-fortigate_rules.xml
0080-sonicwall_rules.xml     0185-vsftpd_rules.xml            0290-firewalld_rules.xml    0395-hp_rules.xml
0085-pam_rules.xml           0190-ms_ftpd_rules.xml           0295-mysql_rules.xml        0400-openvpn_rules.xml
0090-telnetd_rules.xml       0195-named_rules.xml             0300-postgresql_rules.xml   0405-rsa-auth-manager_rules.xml
0095-sshd_rules.xml          0200-smbd_rules.xml              0305-dropbear_rules.xml     0410-imperva_rules.xml
0100-solaris_bsm_rules.xml   0205-racoon_rules.xml            0310-openbsd_rules.xml      0415-sophos_rules.xml
0105-asterisk_rules.xml      0210-vpn_concentrator_rules.xml  0315-apparmor_rules.xml     0420-freeipa_rules.xml
0110-ms_dhcp_rules.xml       0215-policy_rules.xml            0320-clam_av_rules.xml      0425-cisco-estreamer_rules.xml
```

OSSEC環境介紹

OSSEC LOG存放位置 /var/ossec/logs/

1. active-responses.log 存放OSSEC執行主動回應功能的紀錄 (例如將某個符合條件的IP加入拒絕連線清單)
2. ossec.log 系統狀態日誌
3. alerts/alerts.log 存放告警條件被觸發的紀錄
4. firewall/firewall.log 存放防火牆阻擋條件被觸發的紀錄

OSSEC環境介紹

OSSEC server設定檔說明

OSSEC server主要設定檔為/var/ossec/etc/ossec.conf，格式採xml樣式容易閱讀，可試著閱讀設定檔內的描述，推敲出該設定的用途並嘗試修改。

<global>針對ossec告警通知的相關設定，如自行架設stmp server轉送告警訊息，需在此進行設定
<alerts>多少告警等級以上訊息需要寫入alert_log或透過email告警
<remote>開放ossec server接收外部log (local模式不需要)
<rootcheck>定義rootkit check檢查相關設定
<syscheck>定義系統檔案完整性檢查相關設定
<command>Active response相關指令設定
<localfile>Log分析相關設定
<ruleset>啟用或關閉系統稽核條件

詳細說明https://documentation.wazuh.com/current/user-manual/capabilities

OSSEC環境介紹

Active response 主動回應功能

此功能允許系統主動進行防禦而非被動式的監控，讓OSSEC具備入侵預防系統(IPS)功能，主動回應功能可針對**特定規則(rules_id)**或套用**超過特定告警等級以上規則**。

設定檔範例

```
<active-response>
        <disabled>no</disabled>                                  啟用active-response功能,預設值是no(啟用AR)
        <command>firewall-drop</command>                         執行指令firewall-drop
        <agent_id>001</agent_id>                                 規則適用agent_id
        <location>local</location>                               命令在哪執行?觸發事件的主機(local) 或全部主機(all)
        <rules_id>5712</rules_id>                                哪條rule被觸發時要執行此主動回應功能
        <rules_group>authentication_failed</rules_group>         什麼類型的事件群組被觸發時執行此主動回應
        <level>8</level>                                         超過多少等級以上的事件才執行主動回應功能
        <timeout>120</timeout>                                   阻擋時間120秒
        <repeated_offenders>5,10,30</repeated_offenders>         重複入侵者增加阻擋的時間(分鐘)
</active-response>
```

參考文件http://ossec-docs.readthedocs.io/en/latest/syntax/head_ossec_config.active-response.html

OSSEC環境介紹

查看Active response ruleset

less /var/ossec/ruleset/rules/0095-sshd_rules.xml

```
<rule id="5700" level="0" noalert="1">    事件ID 5700,不進行告警
  <decoded_as>sshd</decoded_as>      使用sshd decoder
  <description>SSHD messages grouped.</description>
</rule>
<rule id="5710" level="5">
  <if_matched_sid>5700</if_matched_sid>  前提必須符合事件ID 5700
  <match>illegal user|invalid user</match>  事件觸發條件，符合內容字串
  <description>sshd: Attempt to login using a non-existent user</description>
  <group>invalid_login,authentication_failed,pci_dss_10.2.4,pci_dss_10.2.5,pci_dss_10.6.1,</group>
</rule>
<rule id="5712" level="10" frequency="6" timeframe="120" ignore="60"> 120秒內發生8次即觸發
   <if_matched_sid>5710</if_matched_sid>    前提必須符合事件ID 5710
  <description>sshd: brute force trying to get access to the system.</description>
  <same_source_ip />   必須是同個IP來源
  <group>authentication_failures,pci_dss_11.4,pci_dss_10.2.4,pci_dss_10.2.5,</group>
</rule>
```

系統合規性檢測

什麼是合規性 What is Compliance

公司或機構需採取措施確保其行為遵守相關的法律、法規。

資訊安全合規性要求包含：沙賓法案(SOX)、健康保險可攜性及責任法案(HIPAA)、支付卡資料安全標準(PCI DSS)、聯邦資訊安全性管理法案(FISMA)...等，不同國家與產業會需要不同的合規性標準。

美國政府透過NIST制定政府單位的最低資訊系統安全要求：美國政府組態基準USGCB (United Sataes Government Configuration Baseline)

資訊安全持續性監控

隸屬NIST的國家弱點資料庫(NVD)設有National Checklist Program計畫，公佈多種作業系統及軟體安全性檢查清單，提供SCAP格式及GPO兩種廣泛使用的合規性檢查格式

SCAP (Security Content Automation Protocol)
檢測系統弱點及安全威脅的自動化協定

GPO (Group Policy Object)
內建於微軟NT視窗作業系統用於控制系統環境、帳號權限的系統元件

NCP計畫連結 https://nvd.nist.gov/ncp/repository

資訊安全持續性監控

隸屬NIST的國家弱點資料庫(NVD)設有National Checklist Program計畫，公佈多種作業系統及軟體安全性檢查清單，提供SCAP格式及GPO兩種廣泛使用的合規性檢查格式

There are **9** matching records.

Name (Version)	Target	Product Category	Authority	Last Modified	Resources
USGCB Windows 7 (2.0.x.1)	Microsoft Windows 7 Microsoft Windows 7 x86 (32-bit) Microsoft Windows 7 x64 (64-bit)	Operating System	USGCB/TIS	01/25/2016	– SCAP 1.2 Content - Windows 7 Oval 5.10 - Tested By: USGCB/TIS – GPOs - USGCB Windows 7 GPOs – Prose - This is the human readable version of the USGCB settings.
USGCB Windows 7 Firewall (1.3.x.1)	Microsoft Windows 7 Microsoft Windows 7 32-bit (X86) Microsoft Windows 7 64-bit (X64)	Operating System	USGCB/TIS	04/28/2015	– SCAP 1.2 Content - Windows 7 Firewall Oval 5.10 - Tested By: USGCB/TIS – GPOs - USGCB Windows 7 Firewall GPOs – Prose - This is the human readable version of the USGCB settings.

NCP計畫連結 https://nvd.nist.gov/ncp/repository

自動化合規性檢測工具

NIST認證SCAP工具清單

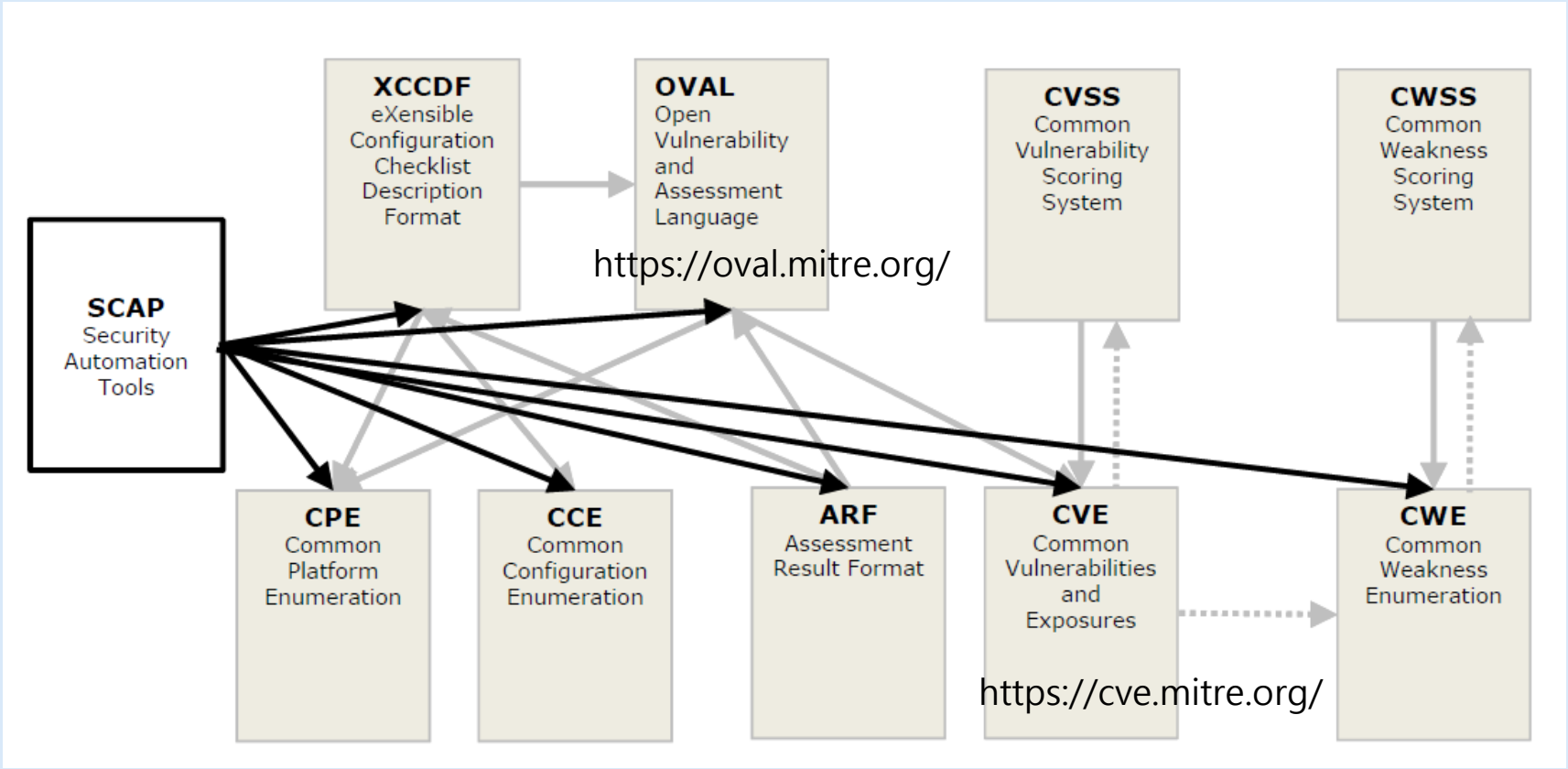
https://csrc.nist.gov/Projects/scap-validation-program/Validated-Products-and-Modules

Linux distribution可使用OpenSCAP

單機版Windows使用微軟Local Group Policy(LGPO)搭配PolicyAnalyzer（傳送門https://goo.gl/5SnNT1)

Windows AD網域納管主機可使用AD或System Center Configuration Manager(SCCM)派送GPO rules

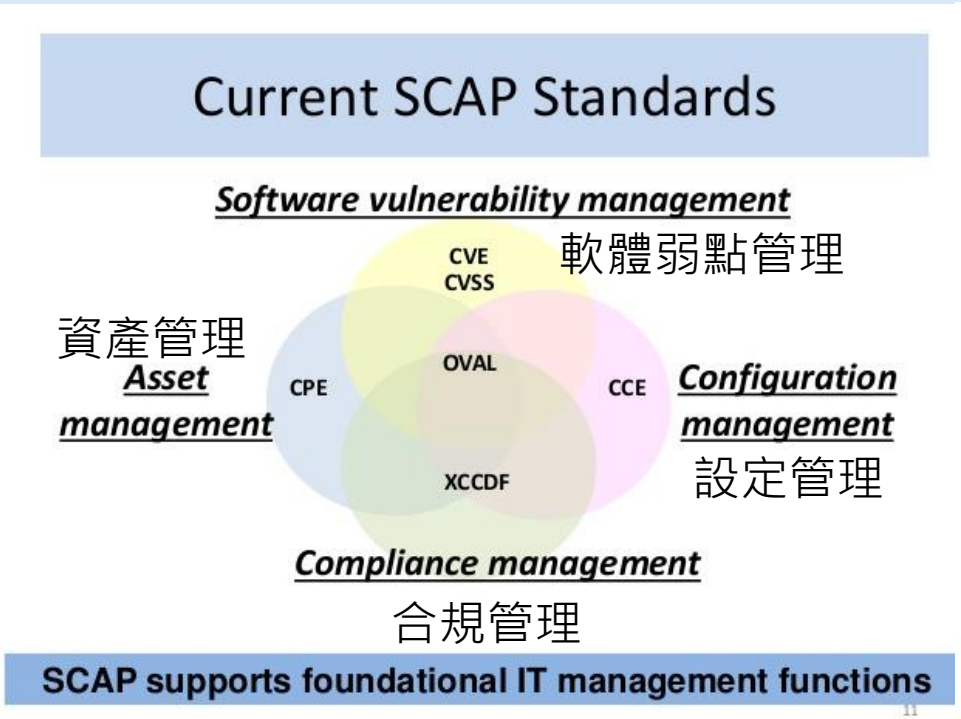
SCAP協定 Security Content Automation Protocol

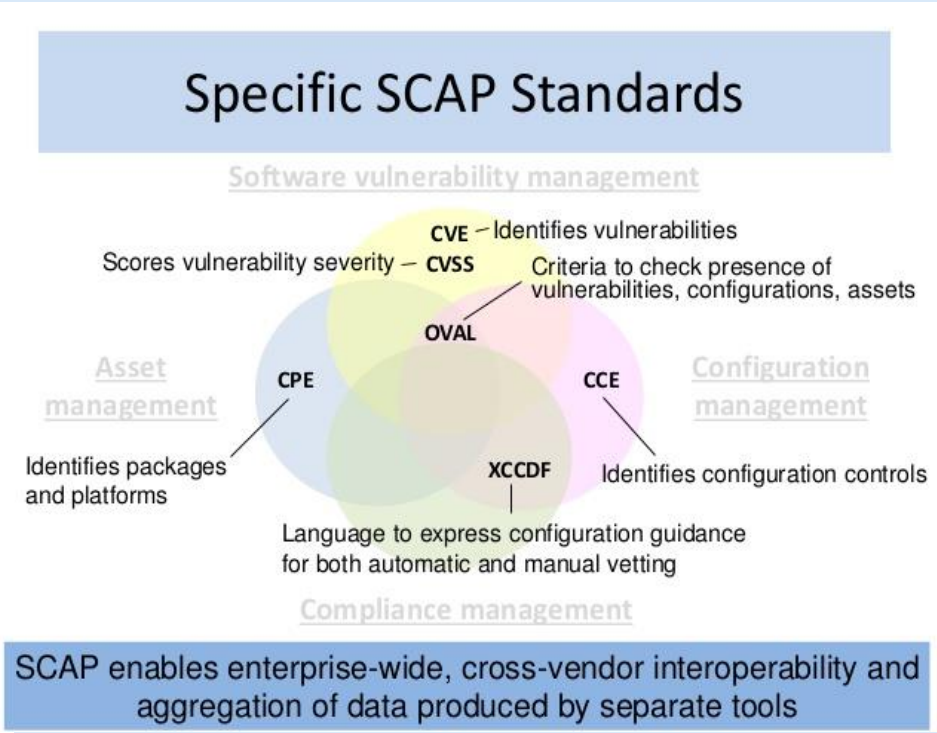


透過SCAP整合眾多安全性設定及弱點交換格式

圖片來源: https://scap.nist.gov/

SCAP協定 Security Content Automation Protocol





圖片來源: http://www.gilligangroupinc.com/

什麼是OpenSCAP專案?

OpenSCAP 專案提供開放源碼框架，讓使用者能整合安全內容自動協定(SCAP) 標準，即時套用最新的SCAP政策及內容，並自動套用調整以符合特定合規要求。

作業系統安全指南 (SCAP Security Guide)
將安全政策轉換為程式可讀取的格式，並可透過OpenSCAP進行稽核、產出報告或將系統套用合規設定，內建國家級與產業標準安全政策如USGCB, PCI-DSS, STIG...等。

OpenSCAP自動安全檢測協定

OpenSCAP Base：執行SCAP設定檢查的工具(被動執行)
SCAP Security Guide：各種規範標準的SCAP設定檔，可供管理者檢測系統合規性
SCAP Workbench：GUI介面的OpenSCAP套件，可客製化進行合規性項目調整
OpenSCAP Daemon：安裝於系統內，排程定期進行系統合規掃描(主動執行)

圖片來源: open-scap.org

OpenSCAP自動安全檢測協定

以Redhat為範例進行OpenSCAP套件安裝、檢測、產出報表

安裝命令列openscap掃描工具

```
# yum install openscap-scanner
```

安裝安全指南

```
# yum install scap-security-guide
```

列出SCAP Security Guide掃描套件

```
#ls -1 /usr/share/xml/scap/ssg/content/ssg-*-ds.xml
```

確認套件內容

```
#oscap info /usr/share/xml/scap/ssg/content/ssg-rhel7-ds.xml
```

進行評估掃描並產出report.html 檢測結果

```
# oscap xccdf eval \
 --profile xccdf_org.ssgproject.content_profile_rht-ccp \
 --results-arf arf.xml --report report.html \
 /usr/share/xml/scap/ssg/content/ssg-rhel7-ds.xml
```

OpenSCAP自動安全檢測協定

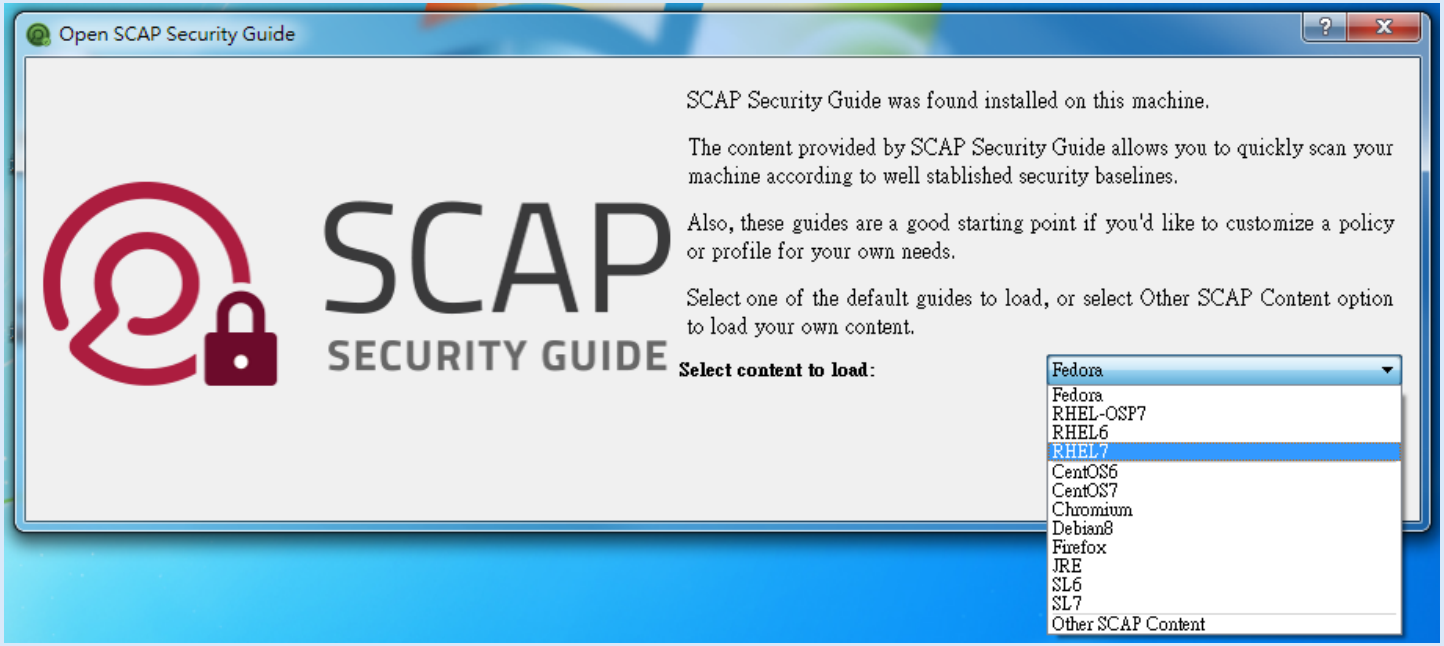
Windows環境發動執行OpenSCAP檢測 (目標僅支援開啟sshd服務的Linux主機)

下載SCAP Workbench 下載連結https://goo.gl/2HxFMT

內建Security Guide包含Fedora, CentOS, Debian, OpenSUSE, RHEL, Ubuntu

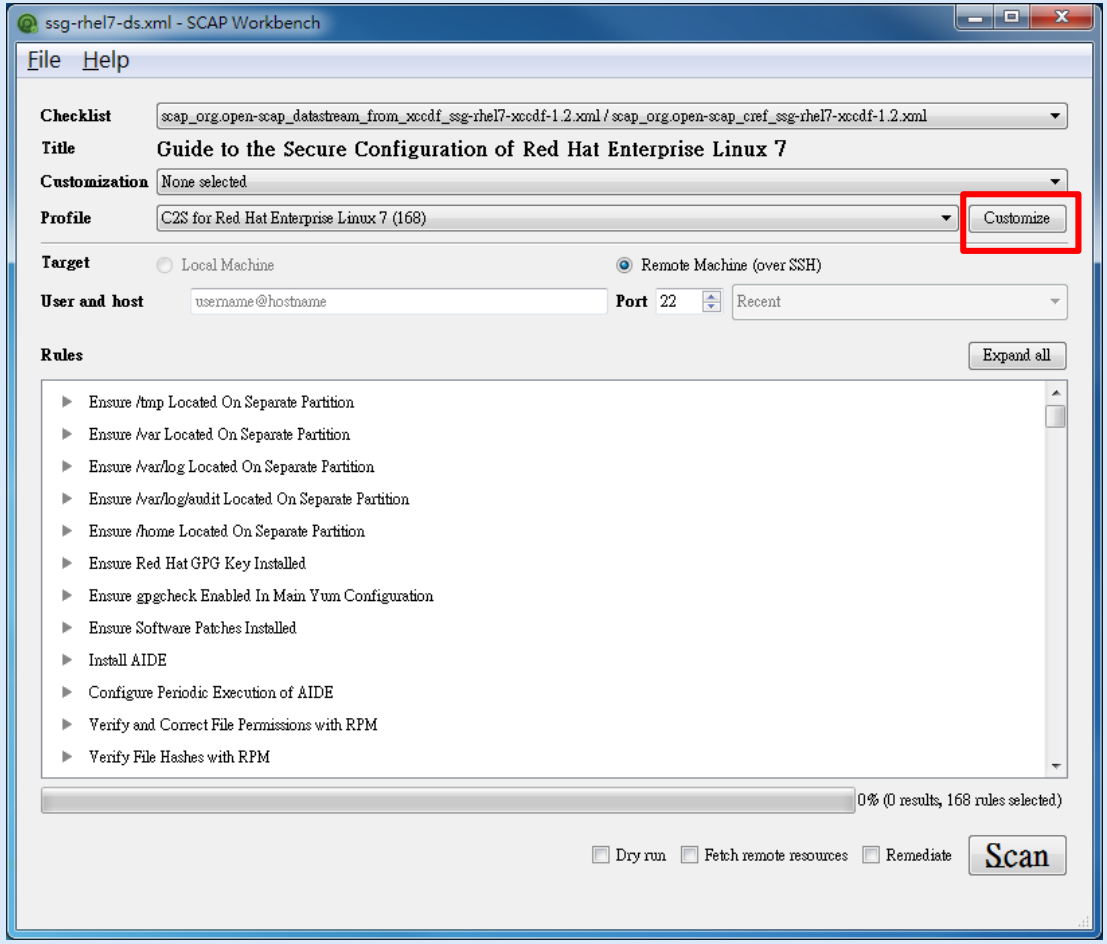
執行scap-workbench-1.1.5-1.msi安裝SCAP Workbench

選擇要掃描的OS環境，此處選RHEL 7，並點擊右下的按鈕Load Content



OpenSCAP自動安全檢測協定

Windows環境執行OpenSCAP檢測操作畫面



Checklist 欲檢查項目 (可省略)

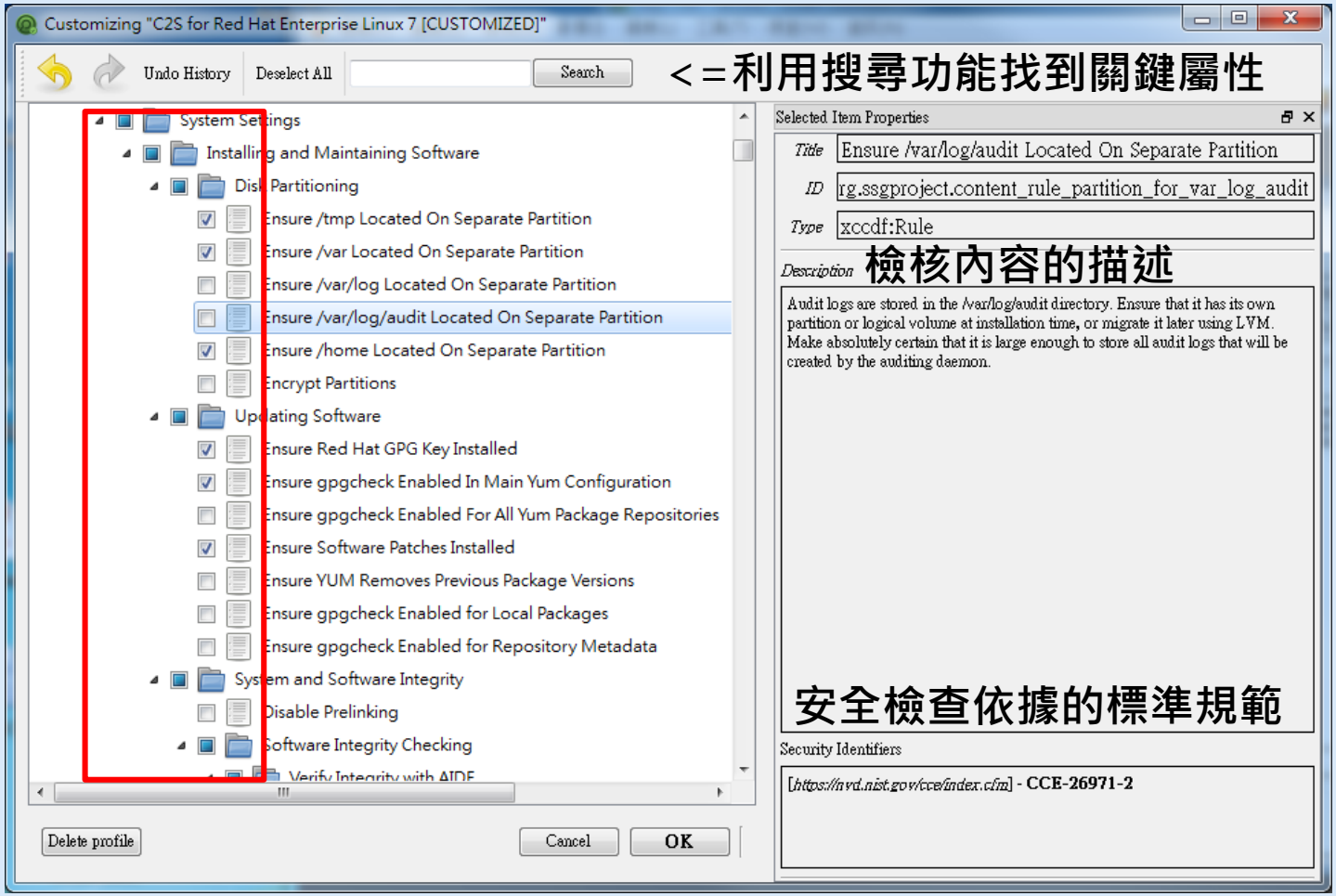
Customization 客製化設定

Profile 選擇進行掃描的設定檔
可點選Customize進行Rules客製化

Target 輸入掃描目標user@host

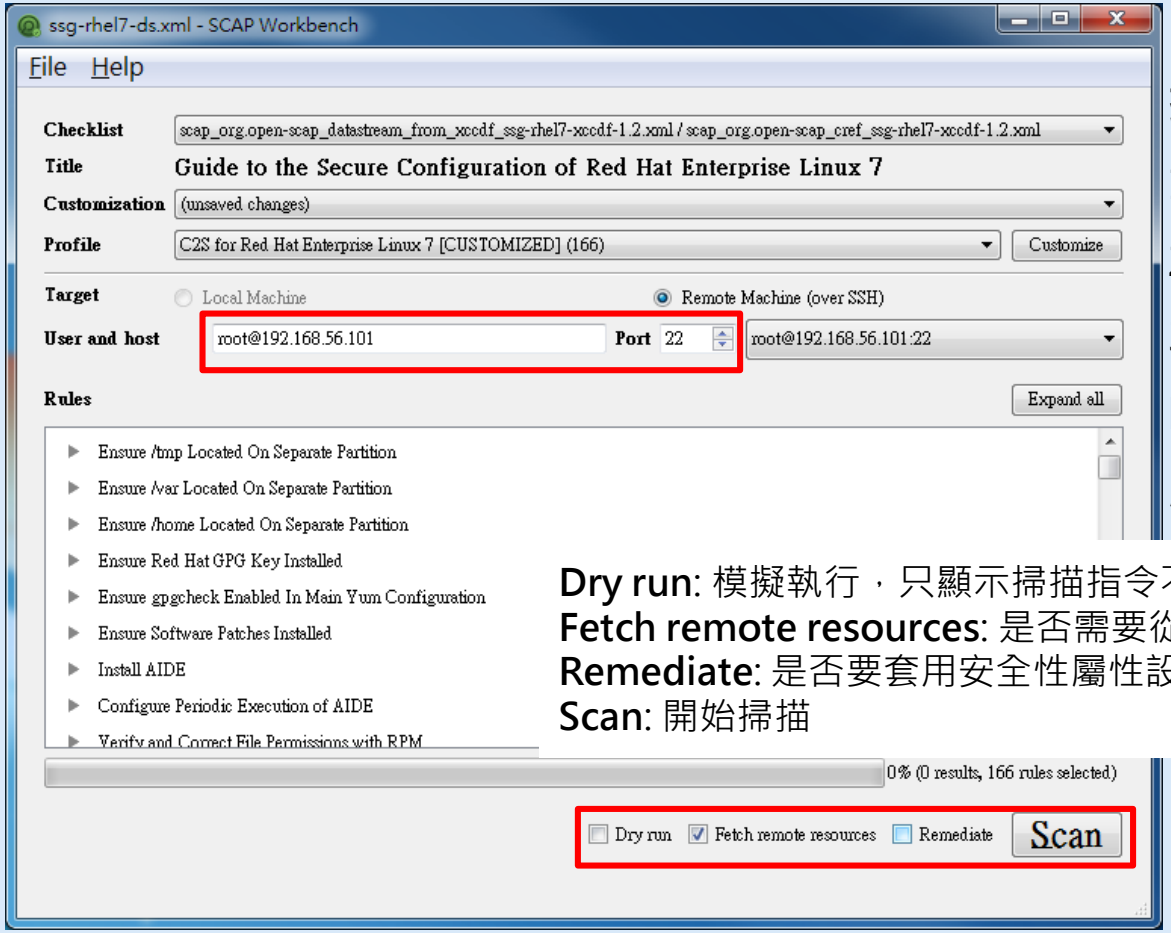
OpenSCAP自動安全檢測協定

針對組織需求修改合規性標準預設Rules，並可另存為新的設定檔



OpenSCAP自動安全檢測協定

輸入掃描標的 user@IP和SSH port，進行Scan



掃描前須確認

1.確認client已設定IP

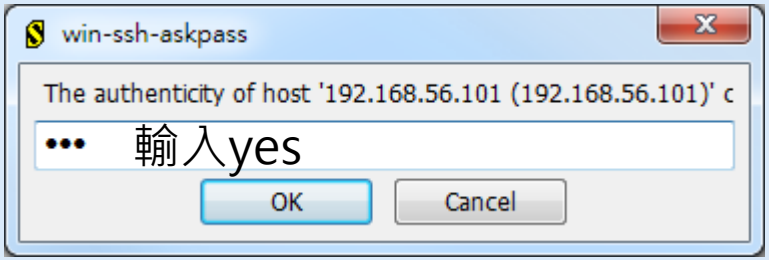
2.防火牆將ssh **tcp/22 port**開啟

3.修改/etc/ssh/sshd_config **PermitRootLogin參數為yes**並重啟sshd

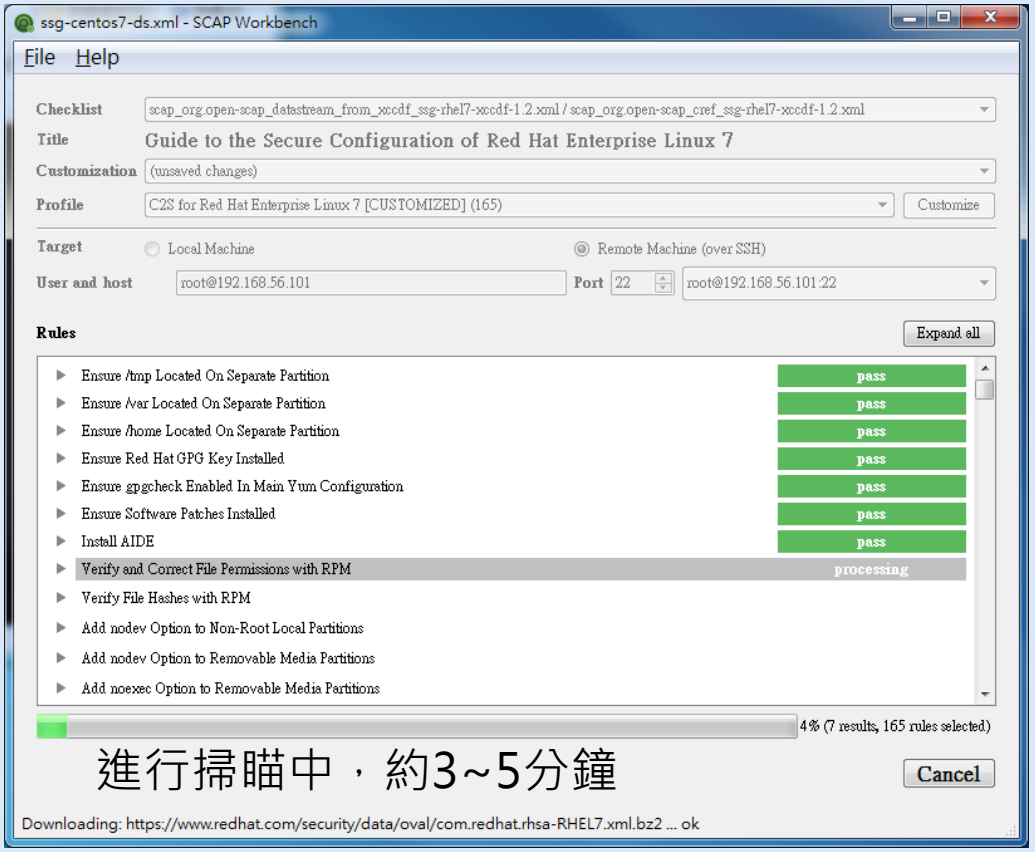
Dry run: 模擬執行，只顯示掃描指令不會真正執行
Fetch remote resources: 是否需要從受檢查端下載SCAP檔案(需連網)
Remediate: 是否要套用安全性屬性設定(線上環境務必先行測試)
Scan: 開始掃描

OpenSCAP自動安全檢測協定

透過SSH對RHEL 7主機進行掃描

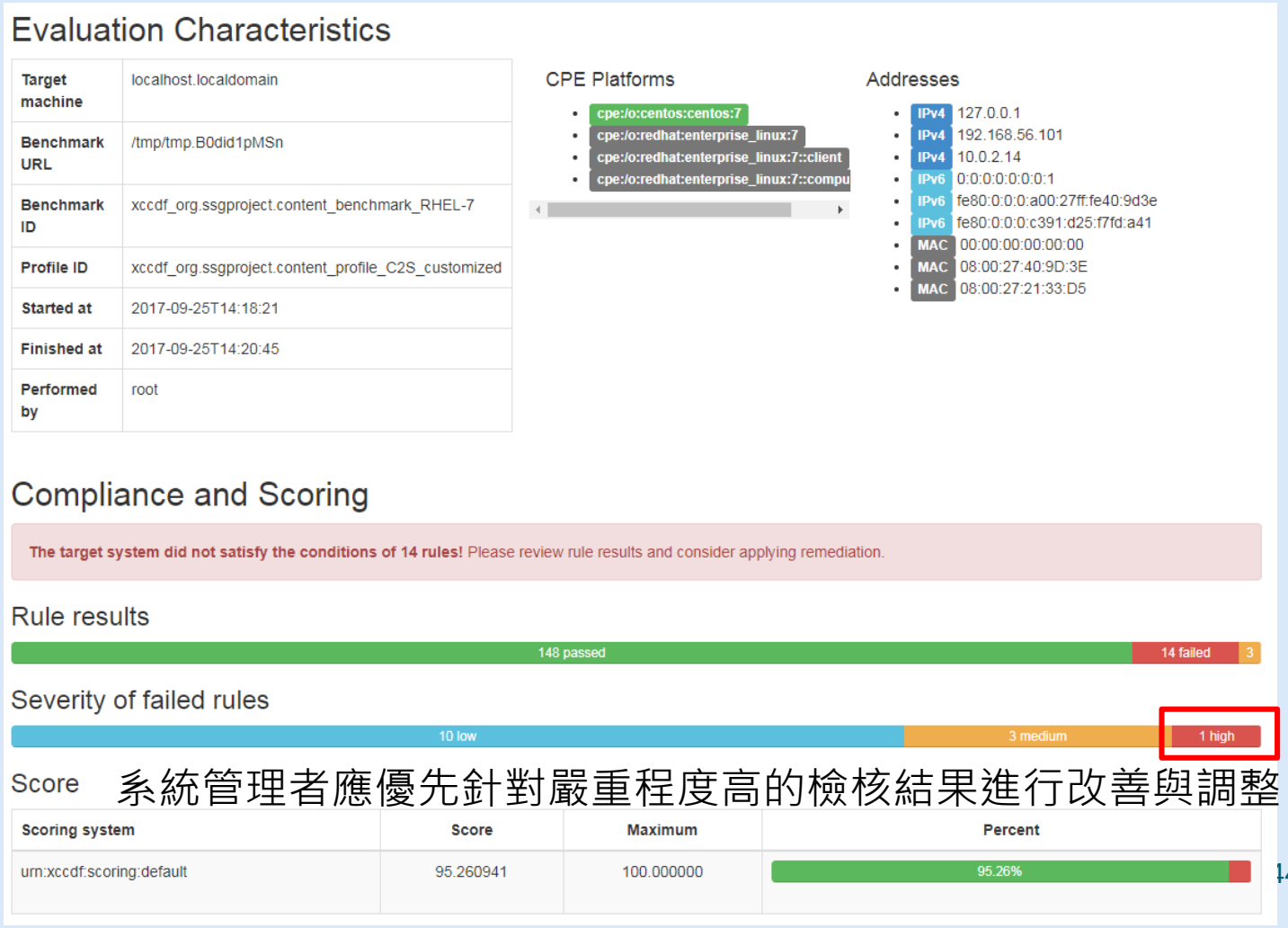


建議採ssh金鑰認證取代輸入密碼



OpenSCAP自動安全檢測協定

掃描結果報告



Evaluation Characteristics

Target machine	localhost.localdomain
Benchmark URL	/tmp/tmp.B0did1pMSn
Benchmark ID	xccdf_org.ssgproject.content_benchmark_RHEL-7
Profile ID	xccdf_org.ssgproject.content_profile_C2S_customized
Started at	2017-09-25T14:18:21
Finished at	2017-09-25T14:20:45
Performed by	root

CPE Platforms

- cpe:/o:centos:centos:7
- cpe:/o:redhat:enterprise_linux:7
- cpe:/o:redhat:enterprise_linux:7::client
- cpe:/o:redhat:enterprise_linux:7::compu

Addresses

- IPv4 127.0.0.1
- IPv4 192.168.56.101
- IPv4 10.0.2.14
- IPv6 0:0:0:0:0:0:0:1
- IPv6 fe80:0:0:0:a00:27ff:fe40:9d3e
- IPv6 fe80:0:0:0:c391:d25:f7fd:a41
- MAC 00:00:00:00:00:00
- MAC 08:00:27:40:9D:3E
- MAC 08:00:27:21:33:D5

Compliance and Scoring

The target system did not satisfy the conditions of 14 rules! Please review rule results and consider applying remediation.

Rule results

148 passed | 14 failed | 3

Severity of failed rules

10 low | 3 medium | 1 high

Score

Scoring system	Score	Maximum	Percent
urn:xccdf:scoring:default	95.260941	100.000000	95.26%

系統管理者應優先針對嚴重程度高的檢核結果進行改善與調整

範例完整報告下載連結
https://goo.gl/9PpHgY

OpenSCAP手冊文件
https://goo.gl/eagQkh

整合OpenSCAP報表至Wazuh入侵偵測系統

編輯wazuh server端設定檔將openscap掃描結果與ossec整合

#vi /var/ossec/etc/ossec.conf

```
<wodle name="open-scap">
<disabled>no</disabled>   從yes改為no啟用open-scap功能
```

#vi /var/ossec/etc/shared/agent.conf 貼入以下內容

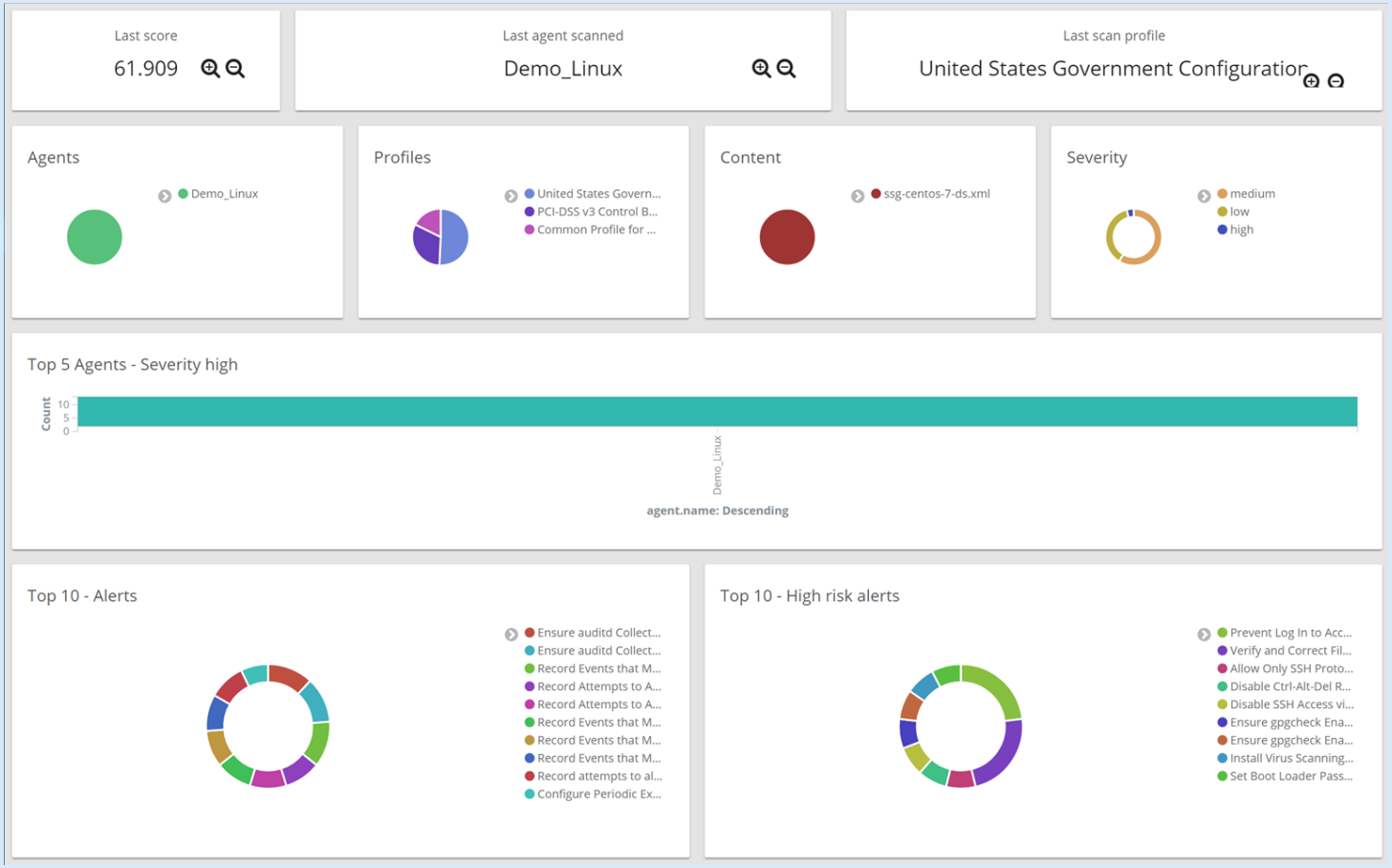
```
<agent_config profile="rhel7">
  <wodle name="open-scap">
    <content type="xccdf" path="ssg-rhel-7-ds.xml">
      <profile>xccdf_org.ssgproject.content_profile_pci-dss</profile>
      <profile>xccdf_org.ssgproject.content_profile_common</profile>
      <profile>xccdf_org.ssgproject.content_profile_ospp-rhel7</profile>
    </content>
  </wodle>
</agent_config>
```

PCI DSS標準
通用設定標準
USGCB標準(Draft)

#/var/ossec/bin/verify-agent-conf　　確認agent.conf語法正確
#/var/ossec/bin/ossec-control restart　重啟server
#/var/ossec/bin/agent_control -R -a　透過server端指令重啟所有agent

查看系統稽核結果

Kibana內的Wazuh APP可看到相關檢查報表



SCAP合規性檢查報表

查看系統稽核結果

Kibana內的Wazuh APP可看到相關檢查報表

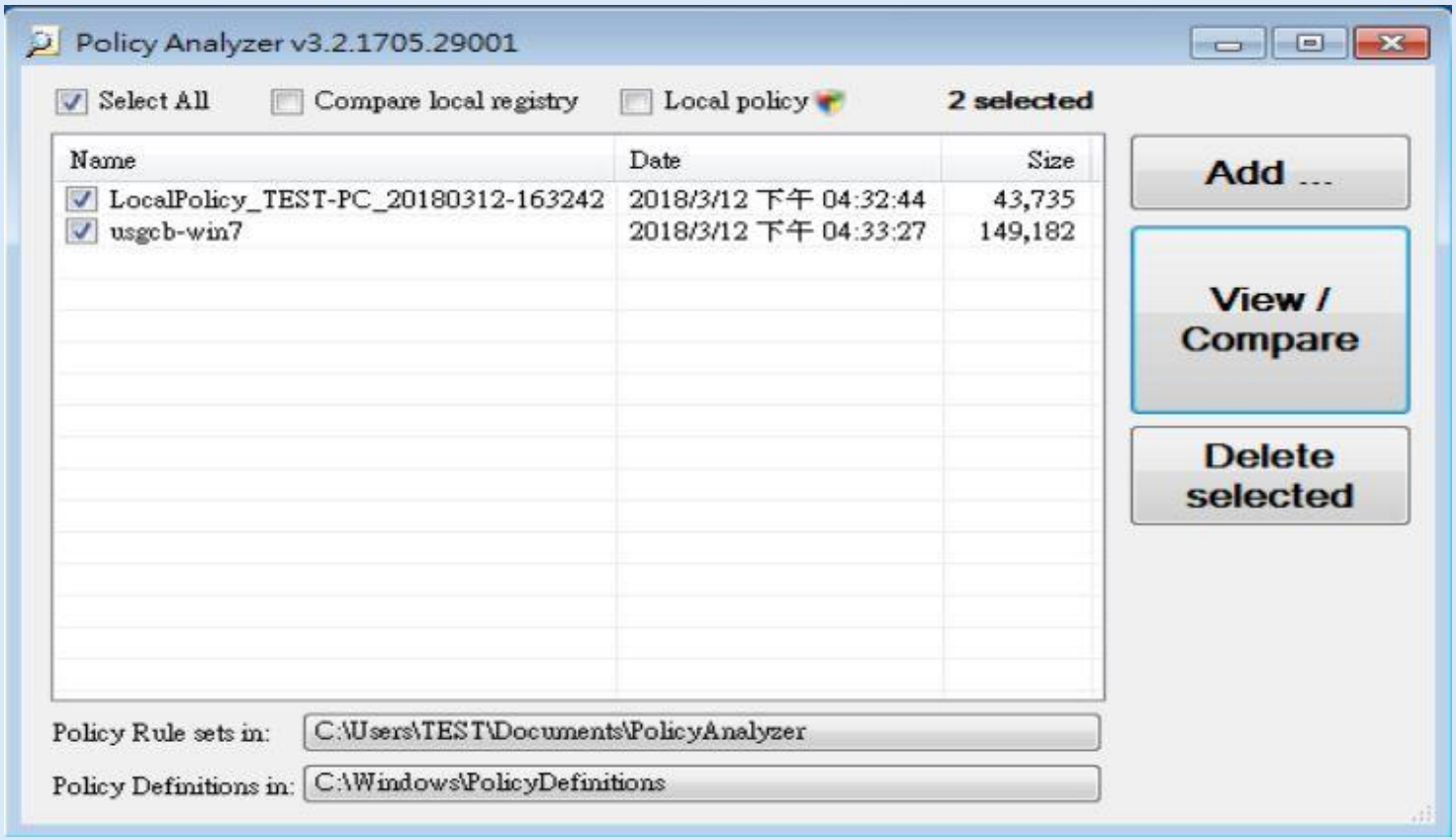
PCI DSS
合規性檢查報表

在Windows環境套用USGCB合規標準

1. 至微軟網站下載LGPO和PolicyAnalyzer https://goo.gl/5SnNT1
2. https://nvd.nist.gov/ncp/repository 下載對應的Windows平臺合規性政策
3. 在測試環境使用LGPO將目標Windows匯入USGCB設定檔進行套用
4. 使用PolicyAnalyzer將測試環境的GPO設定匯出(USBCG template)、正式環境的GPO設定匯出(production configuration)
5. 比較測試環境和正式環境設定，產生出差異檔案
6. 確認修正設定值不會影響線上關鍵軟體，透過組態管理軟體派送至個納管主機套用設定

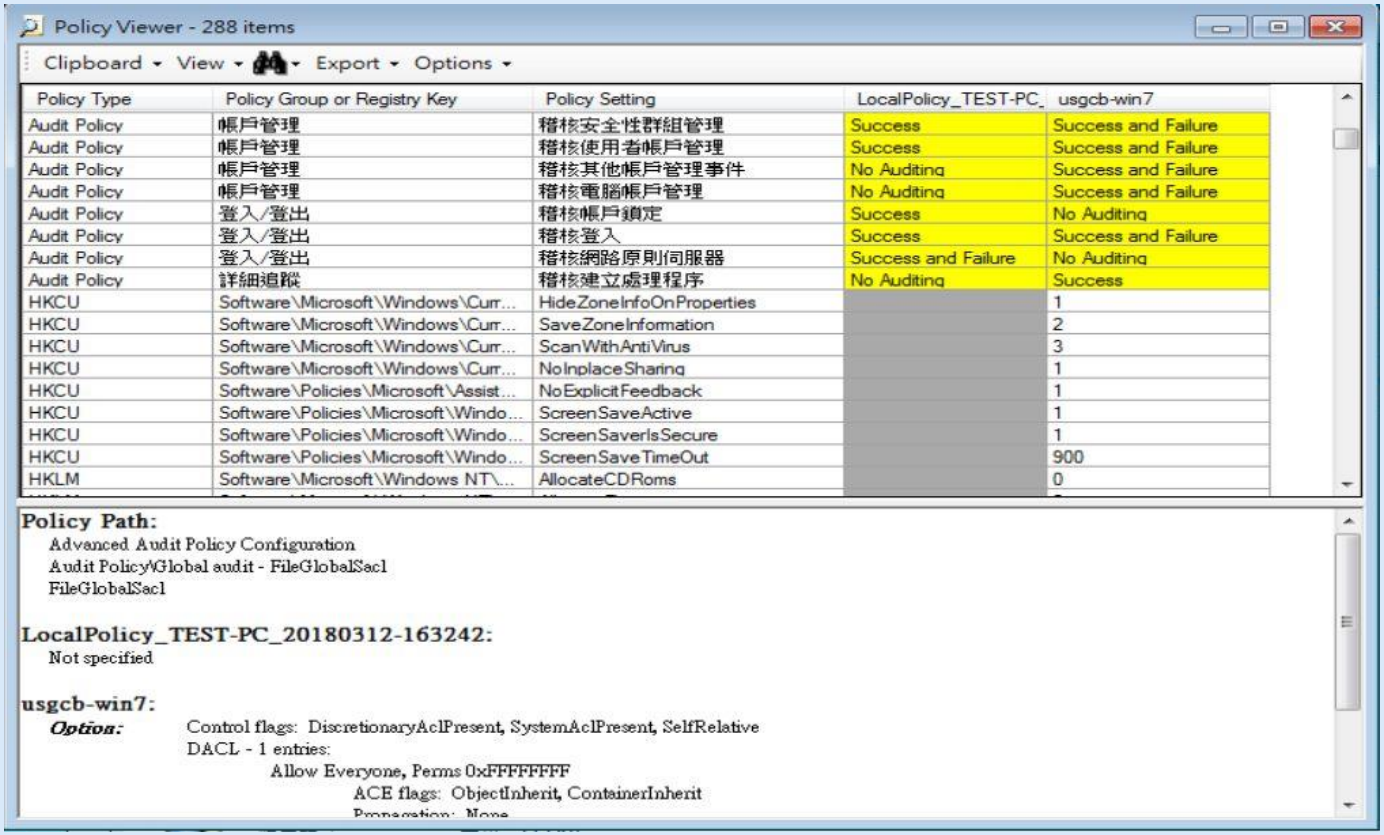
在Windows環境套用USGCB合規標準

產生Windows7測試環境設定檔，並匯入USGCB-Win7比較



在Windows環境套用USGCB合規標準

新安裝的Window7與USGCB 比較結果



在Windows環境套用USGCB合規標準

手動下載、透過組態管理軟體(Pupet,Chef ...)或自行開發PowerShell派送合規組態檔後，以LGPO匯入系統並再將設定匯出與合規組態檔案比對。

Windows AD網域納管主機使用AD或System Center Configuration Manager(SCCM)派送合規組態檔的GPO rules。

以弱點掃瞄工具驗證系統安全性

以弱點掃瞄工具驗證系統安全性

透過弱掃工具檢查系統是否存在有未修補的漏洞或弱點
OpenVAS、Nmap Scripting Engine (NSE)

- 弱點資料庫未必包含最新漏洞
- 弱點掃描結果非全然正確，須詳細評估後排除誤判案例
- 評估弱點是否可形成威脅，依危害程度給予不同風險等級
- 評估內部網路受到攻擊的防護程度(在防火牆內掃描)

結論

- APT威脅無所不在，需假設系統被入侵的前提下監控可疑行為
  - 檔案完整性、資源使用量、程式行為
- 異地日誌匯總+早期預警入侵偵測監看很重要(NIDS+HIDS)
- 不影響重要應用程式前提下，盡快修補作業系統重大安全漏洞
- 單靠防毒軟體+防火牆是過時且消極的防禦方式
  - 已知的特徵值和規則無法阻擋未知的攻擊
- 藉由符合安全性規範的設定加強作業系統的防護能力
  - 正確設定的參數、詳盡稽核軌跡、額外安全機制
- 人是資安環節中最弱的一塊，資安意識的養成很重要

謝謝聆聽

Q & A