2019

MESO RMS
資安風險管理系統

助您追蹤並把關組織內部的資安風險

收納各類系統弱點及網路威脅予以「輕重緩急」來定義其風險指數

風險評估

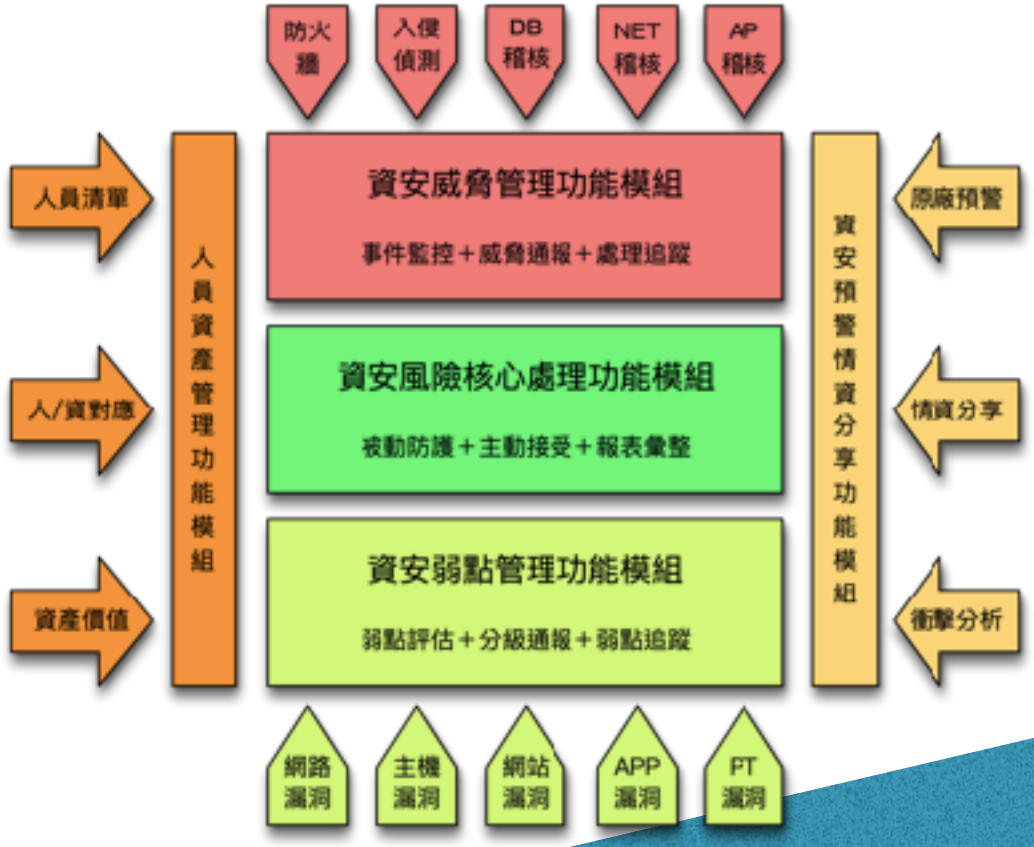
提供資安風險的「完整生命週期」之掃描、評估、過濾、處理及追蹤

弱點追蹤

避免「繁雜紊亂」的資訊傳遞及資安風險難以控管的窘境

資安保障

資安風險完整週期管控
RISK LIFECYCLE MANAGEMENT



ISVMM 即資安弱點管理功能模組
(Information Security Vulnerability Management Module)

弱點管理完整生命週期

1. 掃描結果匯入：支援將多種主流弱點掃描工具軟體所匯出的結果匯入，進行後續彙整評估及標準化的分析處理。

2. 資安風險評估：將匯入之原始資料進行人員及資產的關連及分析對照，並根據風險高低自動分案通報，預設相關修補期限。

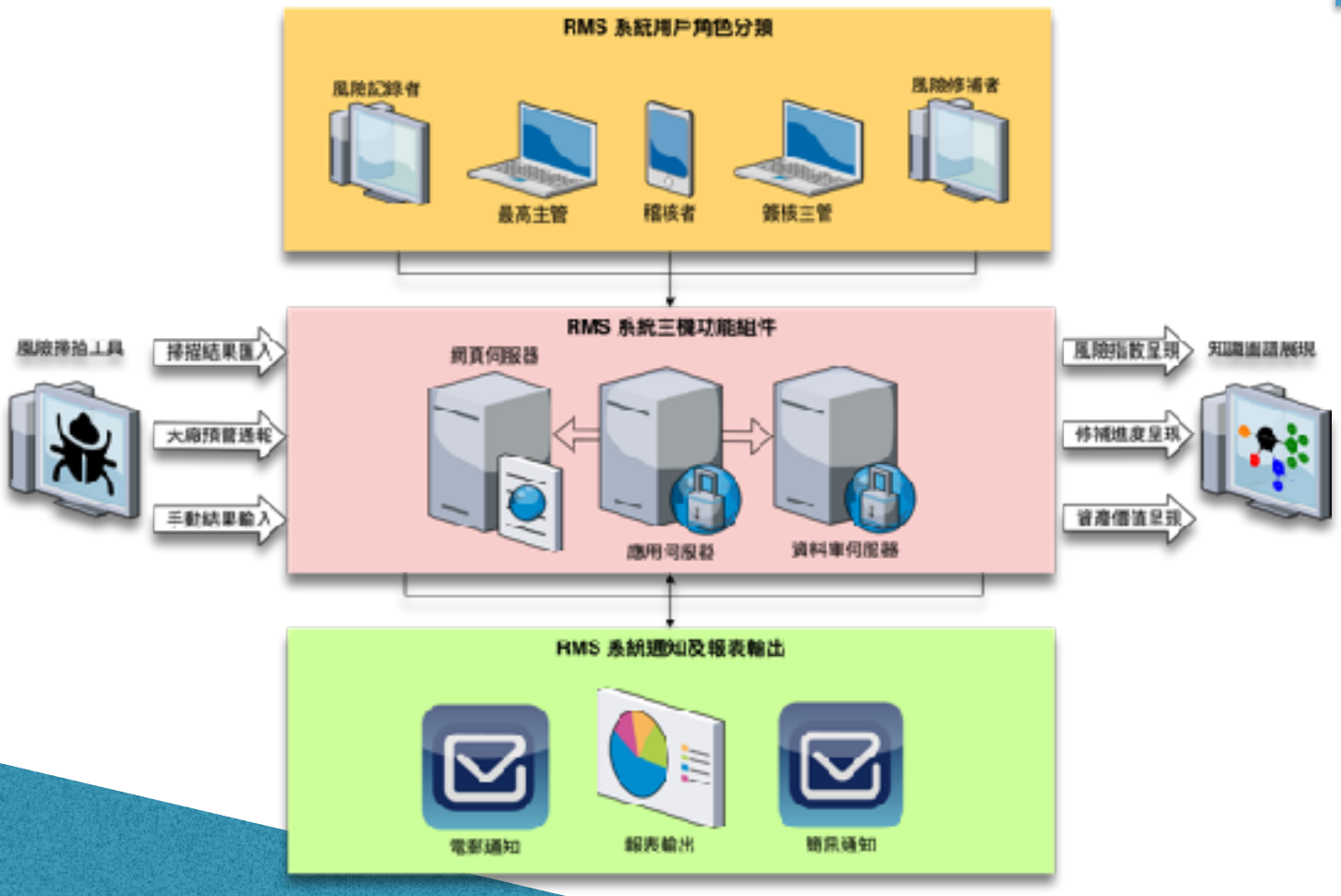
3. 資安風險通報：針對資安風險所屬相關人員，依照風險評估等級以適當頻率與管道進行分別通報，以進入後續修補及處理的系統流程。

4. 修補分派處理：修補人員收到系統通報後，分別進行個案修補及處理動作。或者，將因故無法修補及必須接受的風險記錄後送等待簽核。

5. 處理進度追蹤：修補人員將個別處理紀錄逐一輸入以更新系統進度，審核者也分別將待審記錄作一決策後送或重新指派。

6. 修補完成結案：將已修補或已接受之資安風險事件記錄進行審核以確認結案完成。

資安風險管理系統
ARCHITECTURE OVERVIEW



資安威脅管理功能模組：

可經由不同資安威脅偵測來源匯入相關訊息，例如防火牆、入侵偵測系統、資料庫稽核、網路稽核、應用程式稽核等。

後續並可執行資安威脅事件監控、威脅警示通報，以及相關威脅事件的處理追蹤管理功能。

資安預警情資分享功能模組：

可接受不同來源管道所發佈的資安預警情資，包括：各大軟體原廠預警通報（例如：Microsoft；Adobe；Oracle；IBM 等等）。以及彙整各級政府機關或國安單位所發佈之資安情資分享。

除此之外，還可支援專業資安單位所進行的資安狀況衝擊分析的結果與報告，進行預警情資的通報；分享；記錄；比對；分析；追蹤；修補及回報等等後續資訊處理程序。

配套硬體需求：實體機/虛擬機
- CPU：1.2GHz (雙核) 含以上
- RAM：16 GB 含以上
- HDD：500 G 含以上
- 實際硬體需求數量依所規劃之功能模組而定

配套軟體需求：
- OS：Windows Server 2012 R2 含以上
- DB：MS SQL Server 2008 含以上 或 相容版本
- Web Server：IIS/Apache/Nginx 或 相容版本

弱點工具支援格式：
- 弱點工具：Tenable Nessus, Rapid7 Nexpose 或 相容工具
- 黑箱工具：Acunetix WVS、Fortify WebInspect、IBM Security AppScan 或 相容版本
- 白箱工具：依擴充或客製模組而定

授權方式：
- 單次服務軟體授權
- 短期租賃軟體授權
- 每年年約軟體授權
- 購買軟體授權
- 擴充模組軟體授權：（知識圖譜或白箱工具整合）
- 客制模組軟體授權

MESO RMS: ISVMM

資安弱點管理功能模組

FEATURES

1. 弱掃匯入過濾管理功能

●標準工具匯入：支援主機弱點掃描、網頁弱點掃描 等工具之安全性檢測結果匯入。

-主機弱掃工具，例如：Tenable Nessus

-網頁弱掃工具，例如：MicroFocus WebInspect

●CSV 範本格式：滲透測試結果，提供 CSV 範本，助於滲透測試專案團隊的結果匯入或者輸入。

●手動輸入方式：透過手動輸入畫面，進行安全性檢測結果的輸入。

●安全性檢測(弱掃)結果過濾功能：可以依據指定日期、弱點嚴重性、IP 位址、弱點名稱 以及 弱點編號等過濾條件匯入指定條件之弱點掃描結果。

2. 資訊資產管理功能

●資訊資產屬性：例如： IP位址、主機名稱、埠號、應用程式名稱 以及網址(URL) 等等。

●資訊資產價值：根據每個資訊資產的 ISMS 風險評估結果，定義該資訊資產的價值等級，例如：高中低 等級。

●威脅暴露等級：根據該資訊資產可能遭受威脅攻擊的機率，通常可以依據該資訊資產的網段位置來定義，例如：DMZ 網段區域，則遭受威脅攻擊的機率屬於[高]；如果在 Intranet 則遭受威脅攻擊的機率屬於[中]；如果在實體隔離區，則遭受威脅攻擊的機率屬於[低]的等級。亦可根據貴單位的 ISMS 風險評估或者風險評鑑的分類方式來定義資訊資產可能遭受威脅攻擊的機率高低等級。

●資產管理者：負責進行該資訊資產的管理人員，可能是單位承辦同仁 或者單位委外服務廠商，同時也將是未來要協助進行該資訊資產弱點處理的人員。

3. 人員組織管理功能

●使用者管理：針對風險管理的組織與人員進行基本資料的管理，包含：姓名、帳密、職稱、部門 以及 主管關聯性。

●權限管理：根據使用者角色的不同，賦予相對的權限管控。

●支援使用者帳密的整合，例如：MS AD 目錄服務 或者 LDAP 機制的整合。

4. 弱點處理通報管理功能：

●通報功能：根據弱點項目、資訊資產以及資產管理者三者彼此之間的權責歸屬關聯關係，根據該弱點之風險等級(整合弱點、威脅 以及資訊資產價值)，藉由 Email通報相對資產管理員所負責管理的資訊資產之弱點處理案件。

●弱點處理期限管理：根據該弱點之風險等級以及 ISMS 對於風險高中低的修補規範，進行弱點處理期限的通報提醒與追蹤處理規範。

5. 弱點處理管理功能

●弱點處理回覆管理：提供資產管理者針對該弱點可以處理的方式進行表單管理回復，例如：完成修補、無法修補、接受弱點、延後修補、誤判處理、弱點排除、補償措施 ...等等單一或者批次回覆之弱點處理方式。

●補償措施佐證附件：針對屬於中高風險的弱點，如果未能如期修補、誤判處理、弱點排除 或者 無法修補等等特殊弱點處理情形，提供補償措施說明或者佐證附件的文件管理功能，助於主管簽核或者內外稽核的佐證因應需求。

●主管簽核功能：對於資產管理者已經完成弱點處理工作後，提供其上呈主管流程管理，進行單一或者批次的主管簽核與結案功能。

6. 弱點處理追蹤功能

●弱點處理轉件功能：資產管理者可以因為職掌調整、代理或者差勤，將弱點處理工作移轉給其他人員負責弱點處理。

●弱點處理追蹤提醒功能：針對即將到期或逾期尚未處理的弱點處理工作，根據單位追蹤提醒期限需求設定相關參數，藉由Email 提醒尚未結案的相關資產管理員、主管以及資安應變必要人員。

7. 弱點處理查詢與報表功能

●弱點處理查詢功能：提供可依主機名稱、IP、資產管理員、日期、風險等級、弱點處理情形或混合以上的查詢功能。

●弱點處理報表功能：提供弱點處理統計報表、弱點處理逾期報表、以及資訊資產歷史弱點處理明細報表等等。

8. 知識圖譜呈現功能

提供知識圖譜的可視化介面，以呈現弱點管理之人事時地物之相互關聯資訊。

- 某位「資產管理者」之負責資訊資產與相對弱點角度
- 某台「資訊資產」之弱點處理情形角度。
- 某個「弱點項目」之單位風險衝擊角度。

邁梭科技 Meso Technology Inc.

官網：www.meso-tek.com

市話：+886-2-2393-0126

傳真：+886-2-2393-0136

行動客服: +886-966-518776

E-mail: info@meso-tek.com

地址：100台北市新生南路一段60號5F

Designed by Joey Kuo