AIOps ITSM智能事件服務台

事件流程、設備維護風險管理

NOC 中央事件管理監視平台

ISOinsight 智能營運平台錯誤管理支援事件處理流程稽核、風險分佈鑑識分析(詳述**七、AIOps ITSM智能服務台**)

① 事件的觸發－系統針對異常偵測觸發可支援第三方事件接入進行，並具備大中小分類分級，包含有五大類(設備異常/端點資安/環控異常/效能異常/智能偵測)其中智能偵測需要具備智能型核心引擎，系統預設網路異常偵測如:聯外電路斷線、設備失聯、網路Loop迴路偵測、DHCP/固定IP衝突、IP位置衝突、偽冒ARP、未授權之IOT設備入侵等。
② 事件觸發警報－系統監控觸發事件依據預定義發出警報，警報方式包括：SMS, eMail, LINE notify 或 API, trap模式發送。
③ 事件單/派工單事件處理－可選購EVENT-elite模組授權依據IT資產的營運價值與事件等級進行流程管理。
④ 風險評鑑與稽核－可選購RISK-elite模組進一步以保障IT系統與網路營運的穩定，作為企業IT/OT營運平台風險評鑑的基礎。
⑤ 內建的事件觸發與警報加上選購進階流程管理支援企業完整事件時間戳記、歷史紀錄、知識庫、風險評鑑報告。

關鍵特色

- ISOinsight 多主機同時運算的叢集，統一網路、系統、事件、服務偕同運作監控，告警相關連(Correlation)功能。
- 超級管理者可依據管理員職掌「管理範圍」、「事件類別」進行不同的任務分派功能、負責之事件群組，顯示不同「事件」顯示與追蹤管理。
- 網路與機房設備狀態異常、環境監控臨界值超標、流量、入侵偵測網路安全行為等五十餘種異常檢測事件及告警。以多銀幕與視窗進行提供事件告示與追蹤功能，事件可以設定嚴重等級、定義事件形式與動作,並進行監視、不同層級告警通報、解決、完成處理與過程註記。
- 具備ISO文件報表查詢產出功能，協助管理者每週／月／季／年提出書面報告，內含現況報告、問題說明與調校建議。包括：線上資訊服務可用率、設備運作故障統計與明細分析。
- 事件觸發除了系統內建五十餘種異常偵測情境之外,亦可接收第三方依據特定來源IP syslog或SNMP trap、嚴重等級、關鍵字進行自定義事件觸發與警報方式。

事件類別

① 設備節點錯誤監控: 交換器、路由器、防火牆、伺服器/儲存設備、環控設備(具備SNMP)等錯誤狀態/CPU使用/介面臨界值/錯誤封包
② 網路環境L2/L3/L4監控: IP衝突, IP使用, VLAN廣播，TCP服務反應速率, 惡意DHCP
③ 流量效能異常：骨幹介面流量、IP會談數超標、使用流量Quota超標、會談行為異常。
④ 資安異常監控：MAC/IP未授權、ARP異常攻擊檢測、入侵偵測IDS/IDP聯合偵測。
⑤ 自定義事件：啟動/停用定義那些需要監控、執行事先所定義之程序，集中管理監控網路上設備與的端點異常事件。

事件等級

① 等級定義：依據風險設備等級＋事件等級
② 顏色標識風險：X 紅、黃、綠、
③ 告警等級：依據不同風險建立等級告警

事件視窗與警報

圖八. 2

ISO基礎報表

- ISO稽核報表－線上資訊服務可用率、設備運轉使用良率、IT資產清冊（硬體類、軟體類、服務類）
- 運營報表－網路與系統設備運轉使用狀態、服務水準,電路,組織流量、異常事件訊息等定期統計與稽核報告
- 資安通報－教育部資安通報作業、鎖定名單列表、攻擊與違規異常事件統計與類表
- 無線使用報表－無線設備狀態列表、群組使用排行、AP使用排行、整體無線使用人數與終端屬性分析(周/月/季/年)
- IP與端末設備報表－納管端末白名單,IP、組織流量TopN排名,端末設備IP風險評估與依存關係分析。