

正本

檔 號：

保存年限：

國立中興大學 書函

機關地址：40227臺中市南區興大路145號

承辦人：曾釋賢

聯絡電話：04-22840306-724

電子郵件：jackytsengy2k@nchu.edu.tw

受文者：材料科學與工程學系

發文日期：中華民國113年9月11日

發文字號：興計字第1131200111號

速別：普通件

密等及解密條件或保密期限：

附件：

主旨：為提供本校各單位官網與重要主機基礎資安防護，早期預知異常事件，計資中心提供「SIEM資安告警導入」服務，詳如說明，歡迎貴單位多加利用。

說明：

- 一、配合「高教深耕資安專章—韌性校園」規劃內容，為提升校園資訊基礎建設韌性，本校已完成建置「資安訊息與事件管理（SIEM）系統」，利用主機運作資訊集中分析，早期預知異常事件，可即時提供本校各單位主機資安防護服務。
- 二、依據導入方式，本系統提供功能可包含「網頁置換（檔案異動）偵測監控」及「系統帳號(OS)登入成功/異常監控」告警，以學校所提供之E-Mail公務信箱進行告警信件發送。
- 三、本服務業於本（113）年8月7日召開校園網路連線單位網管會議中公告並開放服務申請，有關會議簡報內容請於網址：「<https://nchu.cc/net>」下載，服務內容請詳見簡報P.33-P.45，歡迎各單位提出申請。
- 四、服務申請表請於「計資中心官網=>表格下載=>12. SIEM資安告警導入申請表」項下下載，其餘申請流程請詳見簡報P.44說明。

五、本服務以單位官網主機為主要服務對象，其他對外提供服務之重要主機亦可提出申請，本中心將視需求官網數量與系統可收容能量狀況進行審核收容納管。

六、需求單位請將申請表送至計資中心進行審核，審核通過後由計資中心提供Agent及安裝說明，並由各單位系統管理者自行或洽所屬網站維護廠商協助設定與安裝。相關申請程序與安裝技術問題，請洽業務聯絡人計資中心資訊網路組曾先生，E-Mail：jackytsengy2k@nchu.edu.tw，電話：04-22840306#724。

正本：本校一、二級單位

副本：



國立中興大學