數聯資安

Information Security Service Digital United

企業資安的守護者

GUARDING THE SECURITY FOR YOUR ENTERPRISE

打造企業數位韌性
資安內化再晉級 ▶▶▶

Information Security Service Digital United

ISSDU

品牌價值

掌握風險　透視威脅　建構安全

數聯資安 讓您心安；全心服務 全力以赴

數聯資安以專業的資安服務團隊、深厚的資安經驗及多元的國際合作夥伴，協助企業建構安全的網路環境。隨著應用需求的多元轉變，結合大數據、AI、雲端等技術應用於資安服務，提供企業完善的資安防護體系。

身為國內資安服務領導廠商，全方位資安服務包含：資訊安全監控、資訊安全檢測、資安治理顧問及資安解決方案。更擁有唯一通過三項 ISO 認證且結合大數據的 SOC 資安監控中心，而服務客群涵蓋政府、金融業、醫療、高科技製造...等各產業。

縱合集團、橫跨領導權威
串聯完整資安防護服務

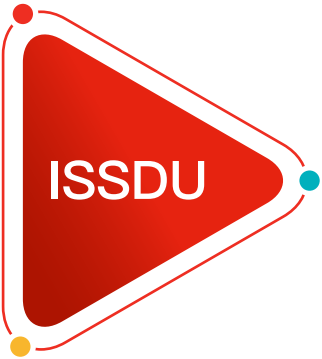
業界第一
以大數據驅動監控

業界唯一通過三項
ISO 認證 SOC 中心

服務優勢

深化力 落實聯網資安

1. 唯一通過ISO認證且結合AI大數據分析的監控中心
2. 熟悉理解資安政策要點，協助企業發展數位轉型



聯盟力 合縱連橫跨發展

1. 整合集團資通訊網路資源
2. 與各界領導權威合作，串聯資安完整防護方案

即戰力 企業首選

1. 擁有300張以上資安專業證照
2. 政府認可優良資安廠商

團隊優勢

市場先行團隊 洞察市場

洞察趨勢應用需求及產業脈動，以豐富的資安經驗與用戶體驗，提供最適切的資安服務及解決方案。

資安規劃團隊 制定對策

以客戶導向的服務及規劃，結合高效與高客製的顧問團隊，協助客戶聚焦並實行量身訂製的資安對策。

技術監控團隊 敏捷運作

以技術底蘊及產業知識發現客戶現行需求，搭配彈性化、敏捷式的團隊協作，為客戶把關與落實資安應用。

數聯資安
Information Security Service Digital United

U-SOC次世代戰情中心

1. 國內唯一且領先以大數據技術並結合情資平台與自動化來強化分析與防禦應處
2. 業界唯一通過三項 ISO 驗證
3. 榮獲政府最新評鑑A級特優殊榮的資安監控廠商

U-SOC次世代雲地聯防監控服務

U-SOC Next Generation Security Operation Center

數聯資安次世代戰情中心能同時橫跨多個公有雲及地端環境，透過大數據及機器學習整合資安設備與系統資訊，進行多重萃取(extract)、轉置(transform)、載入(load)等正規化處理，並匯集到單一監控管理平台內，即時對雲地發生的資安異常威脅事件進行協同關聯分析，並結合資安協作自動化應變(SOAR)、數位情資整合與驗證(明網/暗網/深網情蒐與威脅獵捕)、端點偵測與回應等進階功能，強化威脅偵測時效及回應時效，提供強大的資安監控技術能量與韌性，增強客戶持續掌握組織資訊安全狀態與風險的主動式聯合防禦。

服務優勢與效益

在巨量化事件資料中，即時有效的洞悉新興資安威脅

1 智能化驅動

以大數據平台為核心匯集多元類型資訊，加速進行各類型關聯偵測與分析識別

2 即時智能分析與偵測

透過機器學習提升關聯規則偵測完整性與判讀精準度

3 自動化通報及威脅處置

以自動化應處腳本設定事件通報到結案之流程管控，有效縮短應處時間

4 全方位整合監控

整合多雲混合及地端的日誌收集保存，提升威脅可見度

5 即時比對關聯分析

即時對雲地端發生的資安異常威脅事件進行協同關聯分析與聯合防禦

6 單一監控管理介面

單一介面監控多雲與地端環境，降低管理成本

U-SOC自動化聯防服務(SOAR)

SOC Automation

U-SOC自動化聯防服務(自動化的維運技術)，能依不同客需情境與涵蓋面規劃縱深防禦整合範本，有效達到自動化、偵測、調查能力與即時聯防，降低資安風險並提升維運效率。

服務優勢與效益

1 能擴展整合網端雲

結合情境、設備、系統，減少調查分析的人力耗損，提升回應速度與正確率

2 利用自動化分析威脅事件

利用自動化加以分析威脅事件，並做到二次關聯自動化調查與即時聯防應變處理

3 事件與自動化調查結合

以自動化應處腳本設定事件通報到結案之流程管控，有效縮短應處時間

uSecure RIM 資安風險管理系統

以資訊運營單位觀點為目標，將所有需要進行資安管控的控制項目匯集在一組管理機制的資安風險管理系統，提供營運單位全面性與持續性的風險管理機制。

1. **威脅管理模組 (TMS)：**可將 SIEM/SOAR 平台所匯集檢出的告警與所轄資產進行比對，強化資安威脅事件關聯的有效性。
2. **系統內建的彈性化案件流程機制：**與企業資安維運通報程序結合，將告警傳遞到對應的資產管理人員或其他相關的各部門並回應 SOAR 決行對策，達到即時通報與應處，降低資產風險之目的。

服務優勢與效益

1 彈性化通報跟催流程

具備通報流程編輯功能，可依據企業自訂的管制與稽催程序進行彈性調整

2 整合SIEM/SOAR威脅管理

可支援整合國內主流 SIEM/SOAR 平台的威脅告警案件資訊，提供防護應變的通報處置建議

3 自動產製稽核報表

系統提供排程化產製報告功能，透過內建及客製化的報表可滿足稽核管理之需要

uSecure SIP 資安戰情平台

化繁為簡 掌握資安威脅

透過大數據分析、機器學習及 AI 等技術，高效率萃取更有實質助益的資安情資，並透過容易理解的可視化方式呈現，有效掌握正確資安情資，提升威脅事件的處理效率。

1. **智能化驅動：**透過大數據演算能力搭配智能化事件關聯引擎，從乍看無關資訊發掘並主動列舉未知可能威脅
2. **行為異常分析：**以 AI 規則方法察覺特定裝置中，如大量連線、密碼猜測、異常帳號登入、異常網路連線等行為異常分析
3. **歷史資料回溯：**透過歷史回溯及軌跡資料分析，了解駭客入侵真實特點並提早發現已潛伏的異狀變化
4. **情境感知：**圖像化儀表板及資安天氣圖呈現資安狀態，協助資安管理者提前預測並採取抑制或防範措施

服務優勢與效益

資安情資彙整蒐集，高效資安戰情事件管理

1. 提升資安威脅管理協同作業
2. 提供資安可視化與能見度
3. 提升資安事件管理能力
4. 提升重要資安威脅事件識別準確率
5. 提升資安威脅預測警覺力

數聯資安
Information Security Service Digital United

uSecure Logs 資安日誌收容管理系統

提供完整日誌收容與保存機制，以節省資源且有效滿足組織與企業在資安治理及稽核需求

服務優勢與效益

1 日誌收容，完整保存

- 整合多樣日誌收容管道
- 原始日誌保存完整性

2 分權管理，簡易檢索

- 提供日誌字段全文檢索
- 內建角色權限功能

資安檢測服務

隨著企業資訊化及數位轉型趨勢，科技提升了效率，但也潛藏著資安風險。

若資訊系統中的弱點或是漏洞未加以發現進行修補，則很容易成為駭客的攻擊目標；而組織成員也需要提高資安意識，以防止可能因人為疏失所帶給企業之財產與商譽的損失，所以企業需要藉由事前的各項資安檢測來進行預防動作。

滲透測試

由專業白帽駭客團隊規劃及執行檢測，豐富的攻防演練經驗，模擬網路駭客入侵攻擊時可能發生的各種情況，例如：系統漏洞、程式開發者盲點，或管理者疏忽等因素，可於事前防範檢視駭客可能入侵之途徑與風險。

服務優勢與效益

在巨量化事件資料中，即時有效的洞悉新興資安威脅

1. **專業團隊**
   白帽駭客組成滲透專家團隊
2. **挖掘資安漏洞**
   漏洞深度挖掘
3. **多角度滲透測試**
   多角度滲透測試作業
4. **減輕企業負擔**
   減輕企業專責駭客人力負擔
5. **檢測與諮詢**
   專業檢測報告與顧問諮詢

網站弱點評估

專業服務團隊利用網頁弱點掃描工具，對重要的網站進行掃描，詳細列出網頁應用程式的安全漏洞。更進一步透過專業的弱點分析報表，提供弱點修正及改善建議，協助客戶解決網頁應用程式中存在之弱點，除了能節省客戶花費高額成本購買掃描工具外，更可以有效提升客戶資訊網站安全強度。

服務優勢與效益

1. **專業團隊**
   專業團隊執行檢測
2. **安全性提升**
   提升網頁安全
3. **國際規範**
   國際標準規範
4. **檢測與諮詢**
   專業檢測報告與顧問諮詢

數聯資安
Information Security Service Digital United

系統弱點評估

利用弱點掃描工具，配合其他常用之工具與指令，協助客戶掃描網路環境中各種網路設備與系統主機，快速辨識並修復弱點，包括軟體漏洞、缺少的修補程式、惡意軟體，以及錯誤設定。透過專業的結果分析，提供客戶有效可行的改善方案，藉由弱點掃瞄可提早發現系統維運的安全漏洞，即時完成修補作業，避免藉由弱點遭受入侵攻擊，以達到降低資安風險的目的。

服務優勢與效益

1. **專業團隊**
   專家團隊執行檢測
2. **客製檢測**
   客製規劃檢測
3. **資安弱點分析**
   專業弱點分析報表
4. **檢測與諮詢**
   專業檢測報告與顧問諮詢
5. **安全性提升**
   提升網路環境安全

資安健診

協助政府機關、企業組織進行全面性資訊安全檢視，其中包含：網路架構、網路設備紀錄檔檢視、伺服器主機系統設定、端點防護檢測等不同面向。檢測手法包含實地到場訪談，並使用自主研發之檢測工具及搭配自動化工具進行數據蒐集及結果分析，協助企業掌握整體安全性，並針對可補強部分提供改善建議，以達到降低資安風險的目的。

服務優勢與效益

1. **專家團隊**
2. **豐富資安檢測資源**
3. **嚴選檢測工具**
4. **專業檢測報告與顧問諮詢**

行動應用程式(APP)檢測

行動裝置普及，行動應用程式中潛藏可能資安風險，致使用者處於資料外洩或財產損害風險中。依據 OWASP Mobile Top 10 弱點及經濟部工業局的「行動應用 App 基本資安規範」，由TAF認證 APP 檢測實驗室，可受理開發者的檢測申請，確保開發之行動應用程式符合資安檢測基準要求。

服務優勢與效益

1. **TAF 認證實驗室**
   數聯資安「擁有TAF認證」的資通安全檢測實驗室
2. **專業團隊**
   專業團隊執行檢測
3. **資安強化**
   強化APP安全等級
4. **安全信任提升**
   提升使用者信任及商譽
5. **檢測與諮詢**
   專業檢測報告與顧問諮詢

社交工程演練

電子郵件是企業對外溝通的主要管道，卻也可能成為駭客入侵公司內部的攻擊發起點。駭客透過員工感興趣的釣魚郵件誘使點閱，進而詐騙帳號密碼或入侵員工電腦的行為，導致企業蒙受資料外洩與財物損失。藉由定期之社交工程演練，可提升員工資安意識，降低企業可能的商譽與財物損失。

服務優勢與效益

1. **專業團隊**
   專業團隊執行檢測
2. **擬真化演練**
   擬真化演練範本
3. **資料完整統計**
   完整行為統計資料
4. **報告與諮詢**
   專業報告及諮詢

原始碼檢測

專業服務團隊利用原始碼安全檢測工具，對應用程式以檢視原始程式碼的方式，

經由專業顧問分析檢測結果，詳細列出應用程式中潛藏的安全性弱點。並提供發生原因與專業的改善建議，促使應用程式開發人員可以正確快速的修改程式弱點，強化應用程式之防護能力，避免遭受 SQL Injection、Cross-Site Scripting 等攻擊。

服務優勢與效益

1. **專業團隊**
   專業團隊檢測
2. **國際規範**
   國際標準規範
3. **檢測與諮詢**
   專業檢測報告與顧問諮詢
4. **安全性提升**
   提升應用程式安全
5. **減輕企業負擔**
   減輕企業人力及工具成本
6. **MSP 合作夥伴**
   Micro Focus MSP合作夥伴

DDoS演練服務

政府機關、重要民生服務網站屢受駭客組織發動 DDoS 攻擊，導致網站服務停擺，為加強 DDoS 攻擊的防禦及應變能力，數聯資安 DDoS 模擬演練提供客戶真實、可控的的攻擊演練服務，協助客戶了解當前網站或重要主機承受 DDoS 攻擊的耐受度，並設計防護方案以阻擋 DDoS 攻擊事件。

服務優勢與效益

1. **流量測試**
   合法可控的真實流量
2. **承受度測試**
   及早確保 DDoS 攻擊承受度
3. **專業團隊**
   專業團隊執行檢測
4. **報告與諮詢**
   專業報告及諮詢

雲端組態設定掃描

隨著雲端服務的便利性，越來越多企業採用雲端服務，而雲端服務廠商須負責提供雲端的硬體與底層系統，因而企業用戶往往誤會雲端安全也是服務廠商的責任。但事實上，在雲端共同分擔的資安架構下，組態設定是企業的責任。所以企業應該要有適合的檢查管理機制，針對雲端組態設定錯誤的情況進行調整，以避免可能的資安風險。

服務優勢與效益

1. **專業認證工具**
   使用國際大廠合法授權工具提供服務
2. **組態檢查管理**
   及早發現組態設定錯誤進行調整設定
3. **專業團隊**
   專業團隊執行檢測
4. **報告與諮詢**
   專業報告

資安顧問服務

專業顧問團隊提供 ISMS 資安管理制度與 PIMS 個資管理制度輔導，透過完善管理流程協助企業取得 ISO27001 與個資認證，控制資安風險，保護客戶及關係人重要個資。

ISO 27001 資訊安全管理制度

提升資訊安全管理系統，降低資安威脅與弱點風險，我們的服務優勢與效益：

1. 經驗豐富的顧問團隊：提供客戶貼近需求的最佳解決方案。

2. 預防性控管資安風險：建立資安危機管理及處理能力，快速處理資安事件。

3. 客製化輔導規劃：透過整合方式、最小異動為原則，完成輔導任務。

4. 依循國際管理標準：達到資安保護與持續營運的目標。

服務優勢與效益

ISMS服務除了主管機關、法令法規要求以外，為實現管控自身內部資安議題以及提升同業競爭力的企業提供解決方案，將資訊安全管理制度透過流程式方法進行導入作業，滿足客戶以下需求：

1 資安風險管理

可透過有效管理制度及風險管理，識別出組織內外部相關威脅與弱點並有效降低及管控，發生資安事件時也能快速還原及處置

2 專業團隊

我們的顧問團隊擁有豐富資安經驗，曾輔導過許多不同組織及管理制度證照，能夠提供客戶貼近需求的最佳解決方案

3 資安課程客製化

客製化企業整體資安通識課程，教材包含實際案例分析與年度資安趨勢，提供1~3小時不等之教育訓練，同時符合法令法規要求與提升企業同仁資安意識

PIMS 個資保護管理制度

提升個資保護管理制度，遵循個資法及 GDPR 法規要求，我們的服務優勢與效益：

1.經驗豐富的顧問團隊：提供客戶貼近需求的最佳解決方案。

2.預防性控管個資保護：確保個人資料受到適當保護與管理，以符合法律規範及維護商譽。

3.客製化輔導規劃：透過整合方式、最小異動為原則，完成輔導任務。

4.依循法規及標準要求：協助企業導入完善管理制度。

服務優勢與效益

個資保護管理制度輔導服務除了主管機關、法令法規要求以外，仍有企業為了管控自身內部員工資料及客戶資料，主動積極尋找解決方案，因此個人資料保護管理制度透過業務流程與活動方法進行導入作業，滿足客戶以下需求：

1 個資風險管理

可透過識別個人資料流向，並有效管理個資流程包含蒐集、處理、利用等風險管理，識別出組織內外部相關需管控之處

2 專業團隊與適性輔導

我們的顧問團隊透過個人資料保護法之要求辦理適法性查核作業與現況訪談，讓單位在輔導過程中持續符合標準及法規之要求

數聯資安
Information Security Service Digital United

資安解決方案

數聯資安的全方位資安解決方案，從端點到網路、資料到環境、規範到法規，提供縱深防禦完善的資安防護，協助企業建構安全的網絡環境，有效抵禦新型資安威脅。

MDR 託管偵測與回應

解決資安人力不足及嚴謹的法規要求
持續威脅偵測，並快速調查與回應已確認的資安事件

服務優勢與效益

1 資安整合

全方位整合多項資安設備，輔以EDR做完整性防護，增加SOC事件掌控完整性，並大幅提升應變處理效率

2 自動化判別

協助 SOC 誤報確認、定位威脅、消除威脅、不需人員到點服務、不用等待即時提供協助

3 威脅獵捕與分析處理

專業威脅研究及獵捕團隊，協助進階事件分析、事故處理(ERS)、數位鑑識及惡意程式調查

ZTNA 零信任網路存取

取代VPN連線，讓遠端工作更便利、更安全

服務優勢與效益

1 提高團隊生產力

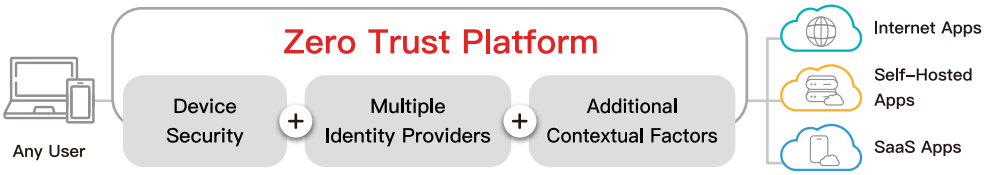
藉由統一的低延遲Zero Trust平台，簡化原則管理、更快速地對問題進行疑難排解，並改善終端用戶的體驗

2 降低網路風險

運用Cloudflare廣泛的威脅情報，防禦多通道網路釣魚和勒索軟體，並縮小受攻擊面

3 提高技術效率

加速數位成熟，並將單點產品與可組合的內嵌式安全服務整合，從而提供全面的網路流量可見度



國際合作夥伴

Cloudflare

全球雲端平台之一，可為全球各種規模的企業提供一系列網路服務 — 使其網路環境更為安全，同時增強其關鍵應用程式或網路資產的效能與可靠性。

CISCO

思科透過五大範疇：資訊安全(Security)、網路創新(Reinvent the network)、多雲環境(Multicloud)、數據能力(Power of Data)，以及用戶體驗(Customer Experience)，協助客戶持續創新，把握數位化的機遇。

Crowdstrike

透過雲端提供服務的次世代端點保護的領導者。唯一整合次世代防毒 (AV)、端點檢測和回應 (EDR) 以及7天24小時威脅偵測服務服務的公司。

f5

基於一個彈性的多客戶共享(multi-tenant)高效能服務架構，讓客戶能夠快速且具成本效益的在任何時候將 layer 4–7 服務配置給任何人，而不會受到任何限制。

Paloalto

具有開創性的 Security Operating Platform 結合了安全性、自動化和分析技術上的最新突破，以持續創新為動力，為企業的數位轉型工作提供全力支援。

Tenable

全球曝險管理公司之一。全球首創的曝險管理平台 Tenable One 能賦予企業的資安團隊隨時洞察整個攻擊破綻的能見度。

數聯資安
Information Security Service Digital United

簡易企業健診

請計算各類別有達成的項目數量，並對應到右側資安成熟度結果

資源面

- 定期編列資安資源預算，以利資安資源運用達成組織對於資安資源要求
- 成立資安小組並落實執行組織對於資安目標要求
- 資訊/資安單位以外之單位已取得ISMS第三方驗證
- 對於利害關係人、團體或關注方之相關資安議題投入資源
- 資安推動小組已訂定標準作業程序並落實執行

管理面

- 資通安全政策、法令及規範等已有因應措施且定期檢視執行情形
- 制定管理程序納入標準作業程序或相關文件化要求，並落實執行
- 落實資通系統及資訊資產之內容，並執行風險管理作業且定期檢視執行情形
- 對資通訊系統服務委外廠商落實執行資安稽核及委外廠商執行之情況調查
- 對資安政策與相關資安活動定期檢討執行情形

技術面

- 定期監控系統架構並持續分析並解決異常行為
- 定期每年辦理技術性服務檢測作業，並持續追蹤弱點修補近況
- 整體資安環境建置完善資安防護措施，並落實且定期檢視其成效與問題修復能力
- 定期備份相關資料與資通系統,並每年檢視其可用性
- 落實資料保護建立控管機制，如DLP防禦、資料加密等方式

宣導訓練面

- 制定資通訊人員教育訓練計畫或指標，並檢視達成之成效
- 每年落實對於主管及同仁之資通安全通識課程至少30分鐘以上
- 資通安全專責人員已取得資通安全或其他管理制度專業證照，並檢視執行成效
- 落實宣達同仁個人電腦使用之資訊安全要求事項，並每年檢視執行成效
- 對於同仁進行資通安全政策、資通安全事件通報流程之宣導作業及評量

資安成熟度

	執行3項以下	執行達3項	執行達3項以上
成熟度	★	★★	★★★
資源面	組織可對於資通安全資源投入更多資源，以利資安防護強化作業	組織視資源運用適當投入資源，以利資安防護優化及補強作業	組織可持續維持資源投入，以利資安持續防護
管理面	組織可依照國際標準建立相關管理制度並委由專業資安顧問公司檢視其內容	組織可強化內部管理制度人員資安專業知識，透過內部人員與專業資安顧問公司協同合作及技術移轉之方式達成管理制度目標	組織可透過外部顧問諮詢方式，持續優化組織內部管理制度要求
技術面	組織可委由外部專業資安公司執行整體資安環境規劃與建議	組織可定期委由外部專業資安公司或內部人員依照既有方式辦理資安防護作業	組織可持續優化並擴增防護範圍，持續落實技術能量
宣導訓練面	組織可委由專業資安公司規劃整體資安宣導並要求落實	組織可依照既有作業模式維持辦理，並檢視不足之處後續強化	組織可透過自動化方式或日常作業活動中納入資安相關議題，可使其活動融入組織中DNA

掌握風險 · 透視威脅 · 建構安全

LINE

OFFICIAL