E-SOFT
曜祥網技

SIP

Security Intelligence Portal

全方位資安智慧平台

精準落實　資安治理

Security Intelligence Portal (SIP)
全方位資安智慧平台-全面落實零信任防禦

全方位資安智慧平台(Security Intelligence Portal)簡稱SIP，是一全面性的自動化管理平台，有效的串聯企業既有的資安管理系統，來達到全方位的資訊資產盤點、弱點風險評估、資安政策合規檢視及矯正自動化作業，讓各個資安管理系統不再是孤島，透過SIP能真正有效落實企業既有的資安管理政策，強化資訊基礎建設的防禦力。

產品特色:

- 旁路設計、無縫式接入不需更改企業既有網路架構
- 專利之ARP偵測封鎖機制(IPv4,IPv6)，在不影響企業網路下可以快速阻擋及解鎖
- 支援客戶各種不同需求之部署架構
- 提供設備完整之資安組態稽核
- 無須在用戶端安裝Agent並採用最小權限設計
- Agentless設計不會增加主機效能及確保主機之整體相容性、穩定性、安全性
- 提供多種存取控制及合規檢查之政策設定(Pre-Check & Re-Check)，並提供自動化矯正程序
- 平台內建資通安全法稽核所需之報表，可因應內外稽核的需求即時產出
- SIP以法規為根基，企業全網資安為核心，進而整合外部網路資安聯合防禦，可以做到事前的預防、事中的因應及事後的處理

零信任架構之
設備存取控制流程

回收
- 設備閒機久未上線回收
- 汰換機回收

盤點
- 人員：帳號/權限/群組
- 設備： MAC/IP/設備種類
- 軟體：作業系統/應用軟體/套裝軟體
- 部署率：作業系統更新/防毒/EDR

覆核
- 防護狀態持續檢查
- 權限最小化稽核檢查
- 系統登入存取控制
- 黑白軟體名單監控
- 定期進行CVE弱點比對

隔離
- 新設備隔離
- 不合規設備隔離

檢查
- 檢查防毒軟體是否安裝
- 檢查設備是否完成掃描
- 未安裝防毒軟體提供矯正
- 即時矯正弱點

申請
- 身份雙因驗證
- 審核授權
- 配發IP

E-SOFT 曜祥網技

SIP全方位資安智慧平台

Dr. IP IP資源管理系統

Zero Trust Architecture

1.自動偵測收集網路所有IP/MAC，找出所有未知資產並產出相對應之設備清單，並提供完整資安管理資訊及報表協助資安維運管理及合規查核使用。

2.管理者可掌握有潛藏漏洞的Windows作業系統設備，並進行漏洞修補及制定對應管理政策。

3.解決企業未授權設備被私自接入公司網路及所衍生之網路相關資安管理問題。

4.IPv4/IPv6雙重協定管理；多樣化的IP/MAC管控政策。

5.IP申請流程自動化。

- 盤點新興科技之裝置清單
- 盤點IoT設備之裝置清單
- 盤點啟用虛擬機之清單
- 盤點大陸廠牌設備
- 盤點老舊系統清單
  (Windows XP,Windows7...)

OA區設備類型

印表機
防火牆
叫號機
電腦設備
網路設備
指紋掃描機
Thin Client
大陸廠牌設備
刷卡機(卡鐘)
電信設備(交換機)

機房設備類型

伺服器
網路設備
IP KVM
IP CAM
DVR 主機
負載平衡器
環控Sensor
刷卡機(卡鐘)

報表 伺服器區IP清單報表

報表 大陸廠牌資訊產品清冊

報表 IoT設備清單

報表 老舊設備盤點

SmartAD 進階管理系統

#Security Analytics
#Privileged Management

一、本機組態盤點

1.網域使用者登出入軌跡管理(可針對一般登入或RDP遠端登入)。

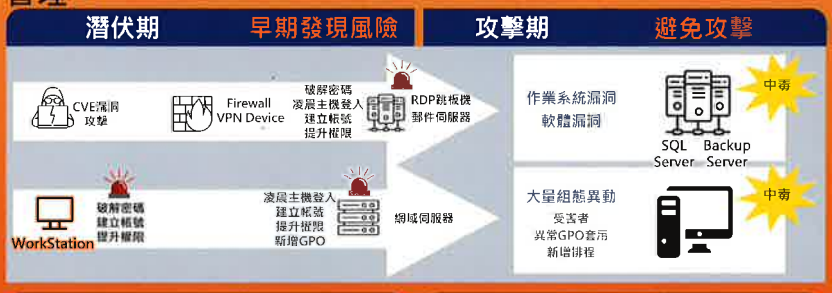
2.檢查設備組態是否存在高入侵風險(Local Admin、ShareFolder、SID重複等)盤點Windows本機使用者帳號、群組、GPO套用等，並記錄其異動資訊。

3.網域設備實名化及網域設備行為異常分析管理。

二、網域組態盤點

1.網域控制站異動稽核分析管理。

2.網域控制站重要物件閒置稽核分析管理。



本機

- 非法時間RDP登入主機
- 本機Guest帳號狀態異動
- 本機高權限群組成員異動
- 本機非法軟體安裝
- 分享資料夾異動稽核
- GCB/GPO套用異動稽核

網域

- 非法時間RDP登入DC
- 網域帳號狀態鎖定
- 網域帳號新增異動
- 網域群組原則異動物件異動
- 網域高權限群組成員異動

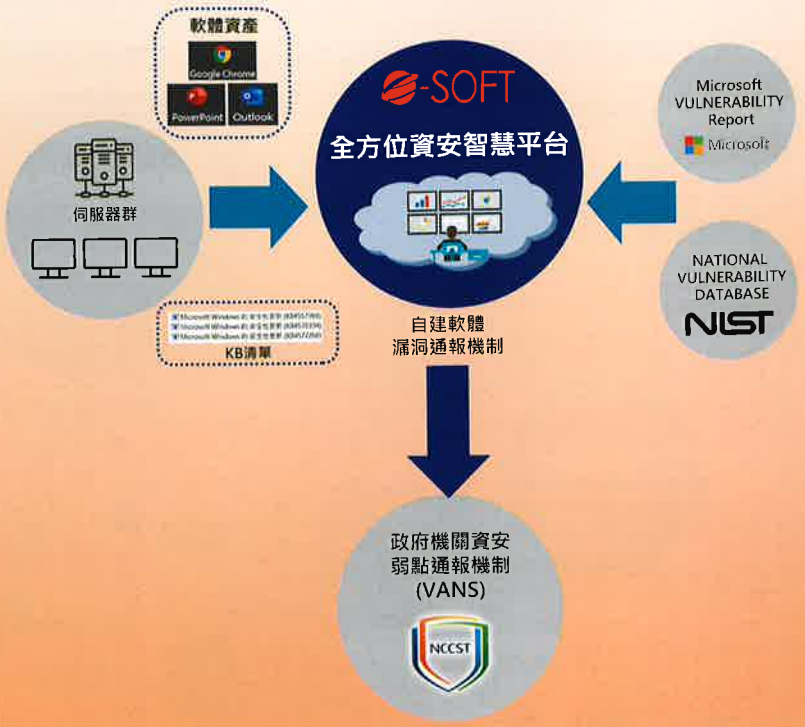
E-SOFT 睿祥網技

政府機關資安弱點通報機制VANS資訊資產系統

資安軟體風險評鑑

Risk Assessment Visibility

1.跨平台完整軟體硬體收集方案
(1)自動化收集Windows安裝軟體資訊
(2)自動化收集Windows安裝KB資訊
(3)自動收集Linux-Like平台安裝軟體資訊
(4)收集交換器的韌體CVE風險盤點
(5)支援行政院技服要求VANS盤點的完整性
(部署率)



2.提供企業自行建立企業軟體漏洞通報系統
(1)軟體資產CPE格式正規化
(2)快速盤點及查詢軟體CVE漏洞
(3)設備軟體CVE漏洞修正派工報表

3.支援政府機關VANS平台上傳
(1)提供手動或自動技服VANS平台上傳機制
(2)提供內外網實體隔離統合上傳機制

連網裝置 收集識別 → 軟體資產 自動盤點 → CPE 正規化 → 軟體漏洞 自我評量

GCB進階稽核管理(政府組態)

GCB

1.內建政府機關可使用之GCB系統強化(Hardening)範本。

2.完整盤點內網Windows平台是否已套用並符合GCB範本的系統強化(Hardening)組態設定。

3.提供群組化功能的GCB組態設定，以協助快速有效完成設定，因應不同部門所需檢查需求。

4.GCB白名單設定，以因應特定系統因業務需求而無法套用GCB時的例外需求。

5.提供已完成GCB套用的符規率報表及其細項，以因應查核時的報表交付需求。

E-SOFT 睿祥網技

NAC++內網資安智慧部署管理系統

#Agentless

1.部署完整性：全面監控企業內部電腦是否都依公司規範安裝Agent，隨時掌控Agent使用狀況。

2.部署有效性：SIP的統一管理介面提供完整即時的資安訊息，管理者能輕鬆掌握資安軟體部署率與政策執行落實度，大量節省管理者檢查及覆核所需之工作時間。

3.自動化矯正方案：橫向整合矯正機制，整合資產軟體達成自動派發機制。

4.資安合規檢查矯正自動化

(1)新設備接入合規預檢機制(Pre-Check)　(2)連網設備合規持續檢查機制(Re-Check)

(3)未合規設備矯正整合機制　(4)封鎖補丁矯正機制

內外網資訊安全聯防系統

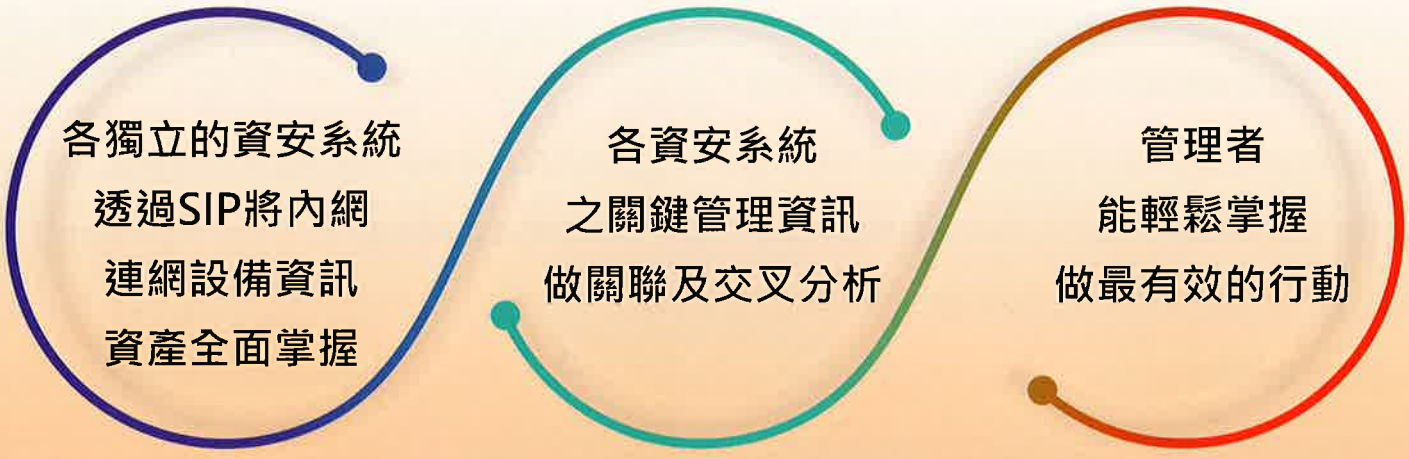
1.SIP與SIEM 資安事件管理產品進行整合後能做到更完善之內外聯防，將SIEM系統具備之資安事件與記錄整合管理功能，提升為具備主動防禦能力的資安管理平台。

2.可與多種品牌之防火牆、IPS、防毒牆之產品進行整合而達到動態防禦的系統協防運作模式，降低管理員必須單台手動設定的負擔。

3.IT部門在人力精簡之情況下，又須面對日益升高的資安攻擊事件的壓力，SIP所具備操作簡易、快速部署、擴充性強、內建全方位的內網資訊與稽核軌跡，可協助輕鬆因應主管機關檢核，將資安防護從網路可視度出發，與現有IT系統及維運做整合，提升整體資安治理的成熟度。

E-SOFT 曜祥網技

Security Intelligence Portal（SIP）



企業導入SIP的效益：

- 協助企業改善內網的設備可視性
- 協助企業快速完成資訊資產盤點覆核
- 協助企業落實各項端點資安軟體部署率
- 協助企業將資訊安全風險評估由被動反應轉化為主動預防
- 快速定位發生資安事件設備之所在，有效縮短資安事件反應時間

客服專線: 0800-333-077
e-mail: sales@e-soft.com.tw
http://www.e-soft.com.tw

E-SOFT 曜祥網技