星擊企業營運資安解決方案

星擊企業營運資安解決方案是一套綜合而高效的資安防禦體系，旨在協助企業應對快速變化的數位環境中所面臨的各種威脅，確保其資產和業務運作的安全性和穩定性。此外，解決方案的特色為我們擁有最專業且高效的資安顧問團隊。透過不斷更新的威脅情報資料庫，星擊資安顧問能夠迅速回應新興的資安威脅，及時調整防禦策略，提高您的企業對於未知風險的應變能力。

方案架構

- 情資、暗網報告服務
- 資安健檢
- 社交工程
- 滲透測試
- 勒索檔案解密

- 資產盤點
- 弱點管理
- 工業協定識別健檢
- OT 資安SOC可視化
- 威脅檢測

- 多因子驗證
- 特權帳號管理
- 資料外洩防護
- 郵件安全防護
- AD 帳號風險管理

- 資安盤點
- 弱點掃描
- 網路流量可視化
- 資安SOC可視化平台
- 網路資安風險可視平台(非入侵)

STARSHOT
星擊科技股份有限公司 Starshot Tech. Corp.
sales@starshot.tw
(03)610 9677
新竹市東區慈雲路118號17F-1

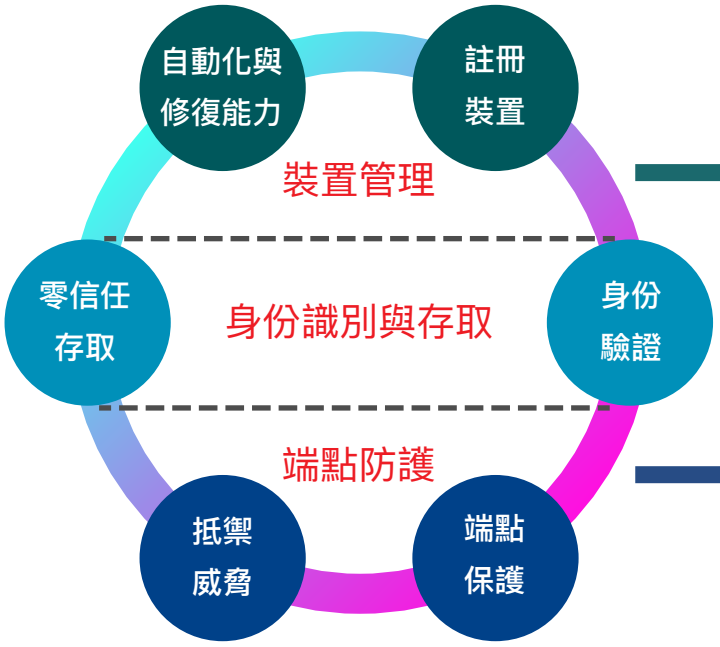
駭客族群分類

供應鏈攻擊　網路間諜威脅　針對性攻擊　國家級駭客攻擊

Check Point 的威脅情報部門指出——2023 上半年的攻擊隨著生成式 AI 的創新與新型勒索軟體的團體而加劇；平均每間台灣企業在上半年遭到 3,245 次攻擊，相當於**每秒1.5萬次網路攻擊**，台灣慘居全球之冠...

面對不斷更迭的新興攻擊，您的企業準備好了嗎？

企業零信任(ZTA)



系統軟體更新、漏洞修補
弱點掃描、管理工具

ERP、MES、APS
多因子驗證工具(MFA)

PC、Sever...
端點、網路偵測系統(MDR)

STARSHOT 星擎科技股份有限公司 Starshot Tech. Corp.
sales@starshot.tw
(03)610 9677
新竹市東區慈雲路118號17F-1

身份驗證與管理

身分識別與存取管理（IAM）： 實施嚴格的身分識別和存取管理措施，包括多因素認證、身分識別驗證和許可權管理。這有助於確保只有經過授權的使用者可以訪問敏感資料和系統。

多因素身份驗證(MFA)

Keypasco Multi-Factor Authentication 是星擊代理之針對網路身份安全防護的統合式身份認證軟體，來自瑞典並與台灣團隊合作研發，擁有多項獨特的多因素身份認證技術，無論是 API 網路平台或企業內部網路，Keypasco都能完整保護存取身份的安全。

滿足使用者需求

- 保護客戶隱私
- 解決密碼管理問題
- 使用者友善操作

安全強度高

- 去識別化技術
- 密鑰分析儲存技術
- 使用者自己掌握
- 有效防止中間人、釣魚、攔截、遠程攻擊等

支援度高

- Web service API 功能完整
- 提供 Cloud 及 On-premise 兩種方案
- 支援跨平台、各種作業系統、常用商業軟體
- 取得國際 FIDO2 及 UAF 認證
- 符合各國法規（電子金融安控基準、GDPR、PSD2）
- 更新、維護輕鬆

國際認證、獎項專利

Keypasco 在全球 16 個國家擁有 5 項技術發明專利，並獲得包括 Frost & Sullivan、APICTA、Red Herring 在內的多個國際獎項肯定；產品應用於電子商務、金融業務、科技製造、e政府、電子支付、智慧醫療、智慧建築、系統整合與供應鏈安全等企業與領域，由此可知 Keypasco 是一套成熟穩定的網路身份安全防護系統，面對後疫情時代高漲的遠端網路需求，星擊科技專業顧問與 Keypasco 將會是您最好的身份認證解決方案。

STARSHOT
星擊科技股份有限公司 Starshot Tech. Corp.
sales@starshot.tw
(03)610 9677
新竹市東區慈雲路118號17F-1

Keypasco MFA 產品特色

- 設備特徵值
- 近場認證
- 時間管理
- PKI 私鑰分拆
- 地理位置
- 智慧風險管理引擎
- 所見所簽
- 防止中間人/瀏覽器或釣魚攻擊

針對網路平台的解決方案

如果您是數位內容服務提供者，擁有龐大的會員

您的會員需要嚴謹的帳號安全及隱私保護,例如金融產業(網路銀行客戶)、電子商務(網購會員)、電子支付(數位憑證)遠距醫療、紅利點管理平台、智慧居家管理平台..等,應用於登入驗證、線上交易、申請憑證、重要訊息更新等等,我們所提供的認證方式,滿足您保護會員的身分認證及數位資產的安全。

網路銀行 | 行動銀行 | 金融科技 | 電子商務 | 電子錢包 | 智慧醫療 | 智慧城市 | E政府

針對企業內部的解決方案

好的系統存取控制與管理措施是您的重要職責

針對企業員工的系統存取控制與管理安全防護，例如一般企業遠距工作、製造業供應鏈、自動化工廠、政府組織等，應用於遠端登入驗證、廠務管理、行政流程管理等等，我們提供多因子認證項目，保護企業與員工各種系統資料存取之身份認證安全。

製造業 | 供應鏈 | 高科技 | 政府機構 | 服務業 | 更多企業

STARSHOT
星擎科技股份有限公司 Starshot Tech. Corp.
sales@starshot.tw
(03)610 9677
新竹市東區慈雲路118號17F-1

雲端郵件管理與協作資安

企業上雲已是現在進行式，越來越多公司選用微軟 o365 或 Google G-Suite 作為員工電子郵件收發與管理系統，讓員工可隨時隨地收發信件。隨著生成式 AI 的發展，網路攻擊變得更多且更聰明，且**根據 PurpleSec 的統計高達 92% 的惡意程式採電子郵件作為攻擊路徑**，如：釣魚郵件、惡意附件、商業郵件詐騙(BEC)、帳號盜用等；內部威脅如：員工洩漏機敏資料、員工對內部同仁發起釣魚攻擊等；各式 SaaS 服務威脅如：Microsoft Teams、Slack、Onedrive 與 SharePoint 等。

業界首創的使用者、裝置與存取權限統合安全防護解決方案

- 獲得專利的 AI 技術，可在郵件進入收件匣之前阻止攻擊
- 5 分鐘設定完畢，無需任何部署
- 與現有工具並行工作
- 適用於所有雲端電子郵件和協作平台
- 提供預防和交付後保護
- 由 ThreatCloud AI 提供支援

全面保護

對雲端電子郵件和協作應用程式提供全面保護，可保護敏感業務資料（DLP）並確保所有業務通訊線的安全

防彈資安

基於應用程式開發介面（API）的解決方案，可捕獲其他人遺漏的攻擊，包括勒索軟體、帳戶盜用、BEC 和供應鏈攻擊

卓越的捕獲率

到達收件匣的網路釣魚攻擊減少了 99.2%，阻止率比雲端原生資安高 30%

為何選擇 Harmony HEC?

1. HEC 是當今最先進且增長最快的下一代電子郵件安全解決方案
2. HEC 專為雲端電子郵件環境而設計
3. HEC 是唯一一個不僅能檢測/回應威脅還能防止威脅進入收件匣的解決方案
4. HEC 設計可與 O365、G-Suite、Slack、Teams 等平台配合使用
5. HEC 與所有其網路和安全工具兼容

STARSHOT 星擎科技股份有限公司 Starshot Tech. Corp.
sales@starshot.tw
(03)610 9677
新竹市東區慈雲路118號17F-1

次世代資安可視性解決方案

次世代資安解決方案是一套將網路防護（NDR）、端點防護（EDR）、使用者行為分析（UEBA）的整合性軟體，可做到透過 AI 核心技術進行跨源整合分析的產品，提供客戶自我防護來自外部的威脅。

法遵需求與國際資安認證

上市(櫃)公司資通安全管控指引 & ISO 27001

管理面

- 成立專責單位
- 訂定資安目標與計畫
- 訂定管理規範與演練
- 權限劃分與管理
- 資安事件應變與回應
- 證據收集與調查

技術面

- 合規性檢測與修補
- 資安防護控制措施
- 威脅偵測管理(SOC)
- 資產管理與監控
- 作業環境區隔管理
- 帳號與資料存取控制

訓練面

- 風險評估
- 資安稽核
- 資安教育訓練
- 資安計畫演練
- 資安專業課程訓練

立即整合資安可視性，讓勒索止步

人工智慧分析

預判攻擊危機

洞悉威脅全貌

科技業資安攻擊數量不斷增加...

2022年
科技業平均遭駭天數高達
332 天
*相比 2021 年成長 25%

2023 上半年
台灣遭受惡意攻擊每秒
1.5萬 次
資料來源：iThome CIO大調查

STARSHOT
星擎科技股份有限公司 Starshot Tech. Corp.
sales@starshot.tw
(03)610 9677
新竹市東區慈雲路118號17F-1

資安監測中心日常運作流程

整合資安可視性、落實縱深防禦的關鍵

- 資安監測中心(SOC) 是即時、集中匯整企業資安訊息的單位，保護企業免受駭客攻擊。
- SOC 是調查重大資安事件的基礎， 能協助事後調查與取證。
- 需針對右方日常運作各項目建構合適的資安工具，並建立標準作業程序(SOP)。

EXPLAINABLE VISIBILITY & RESPONSE

可解釋的威脅告警與跨源威脅獵捕

跨源威脅獵捕

- 端點威脅獵捕
- 網路威脅獵捕
- 使用者異常行為分析

資產合規監控

- 軟硬體組態資訊
- 網路連接狀況
- 外接儲存裝置偵測

證據與調查

- 原始行為及日誌存證
- 全域搜尋、篩選、統計
- 時序圖及樹狀圖分析

STARSHOT
星擊科技股份有限公司 Starshot Tech. Corp.
sales@starshot.tw
(03)610 9677
新竹市東區慈雲路118號17F–1

Woodpecker XVR
功能介紹

端點威脅偵測與回應

惡意行為偵測
- MITRE ATT&CK 資安框架
- 惡意指令執行
- 橫向感染
- 惡意特權提升
- 勒索軟體

資產監控
- 效能監測
- 安全性監測
- 裝置活動紀錄
- 合規性偵測
- 軟體、硬體
- 安全性更新

自動威脅補救
- 受感染裝置隔離
- 惡意程序終止

整合威脅情資

外部情資比對 快速發現已知威脅
- 釣魚網站 IP、Domain
- C&C 伺服器 IP、Domain
- 惡意程式雜湊值

整合開放威脅情資平台
- OTX (Open Threat Exchange)
- MISP (Malware Infromation Sharing Platform)

外部情資自動更新與管理

支援 TAXII 1 / TAXII 2 交換機制

網路威脅偵測與回應

網路攻擊行為分析
- MITRE ATT&CK資安框架
- 資料外洩
- 網路偵察行為
- 殭屍網路攻擊
- 分散式阻斷服務攻擊

網路流採集與檢索
- 輕量化採集
- 流量數據分析搜尋

裝置探索
- 未知裝置探索
- 網路拓樸圖視覺化

跨源整合分析

跨端點與網路的整合威脅分析

高解釋性
- 整合 MITRE ATT&CK 框架提供事件根因時序圖

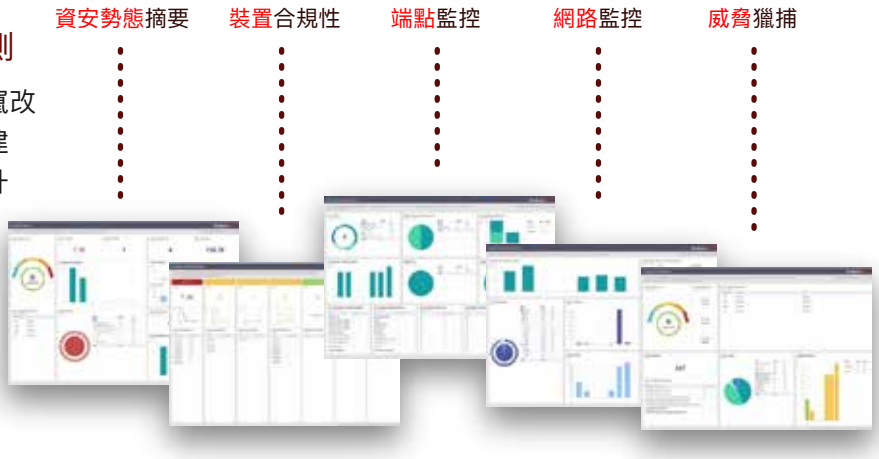
資料可控
- 本地部署資料不上雲
  保障機敏資料隱私

使用者與設備行為分析

異常行為偵測
- 可疑檔案傳輸
- 可疑通訊埠偵查
- 密碼潑灑攻擊

罕見事件偵測
- 敏感登錄檔竄改
- 可疑腳本創建
- 可疑權限提升

異常時間及關聯性偵測
- 可疑登入活動
- 可疑網路連線



STARSHOT
星擎科技股份有限公司 Starshot Tech. Corp.
sales@starshot.tw
(03)610 9677
新竹市東區慈雲路118號17F-1

Active Directory 安全防禦

Active Directory（AD）是由 Microsoft 開發的一個用於管理和組織網路中的資源和服務的目錄服務。它是一種目錄服務，可以用來儲存和檢索網路中的資訊，包括使用者帳戶、電子郵件地址、列印機與電腦，甚至是雲端系統與應用程式。星擊代理的 Tenable Identuty Exposure(前稱 Tenable.ad)是一套快速且無代理程式的 Active Directory 安全解決方案，能夠協助您在錯綜複雜的 Active Directory 環境中洞察一切、預測並降低潛在風險，並且在攻擊者利用這些弱點前就消除攻擊路徑。

Active Directory 遇到的安全問題

在攻擊發生之前尋找並修復 Active Directory 弱點

使用 Tenable 的身份風險評分來發現 Active Directory 中的暴露並確定其優先順序。透過逐步補救指導降低您的身分風險。

即時偵測並回應 Active Directory 攻擊

偵測 Active Directory 攻擊，例如 DCShadow、暴力破解、密碼噴射、DCSync 等。Tenable Identity Exposure 透過攻擊洞察豐富您的 SIEM、SOC 或 SOAR，以便您可以快速回應並阻止攻擊。

STARSHOT
星擊科技股份有限公司 Starshot Tech. Corp.
sales@starshot.tw
(03)610 9677
新竹市東區慈雲路118號17F-1

完整 AD 風險可視化

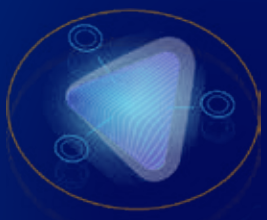
找出 AD 錯誤設定及不適當的權限

立即發現、繪製現有的 AD 風險
遵循我們的逐步補救策略並防止攻擊

AD 管理員　藍隊＆稽核團隊

AD 原生 API 對接

即時分析



不需要特殊權限

雲端＆本地部署

無須安裝 Agent

7x24 持續監控

持續監控 AD 上的物件變化
發現異常狀況即時告警

AD 管理員　資安團隊

調查事件和回溯威脅

在對象和屬性級別搜索和關聯 AD 設定更改
在你的 SOAR 觸發反應

SOC 分析團體　攻擊溯源團隊

即時檢測正在進行的攻擊

獲取有關 AD 攻擊警報和可操作的補救計畫
助 SOC 團隊在 SIEM 中可視化通知和警報

SOC 分析團隊　資安團隊

1 無需代理程式、無需特殊權限、沒有延遲

無需代理程式和特殊權限，就能防止並偵測複雜的 Active Directory 攻擊

2 涵蓋雲端

Serice、AWS Directory Service、或 Google Managed Service for Active Directory 的安全性

3 在任何地點部署

Tenable.ad 提供兩種不同架構設計的彈性。內部部署能讓您將資料保留在現場，並且在您的控制之下。軟體即服務 (SaaS) 則能讓您運用雲端。

消除攻擊路徑

攻擊路徑指的是攻擊者成功利用環境中不良的網路安全而獲利的途徑。Tenable 藉由結合風險型弱點管理與 Active Directory 安全性，能讓您消除攻擊路徑，確保攻擊者難以找到立足點，也無法採取下一步行動。

初始立足點
透過網路釣魚或弱點

攻擊路徑

探索
在目標環境中橫向移動

提升
取得特殊權限存取

迴避
隱藏鑑識足跡

建立
安全程式碼永久立足

洩漏
洩漏資料或綁架目標以便勒索

STARSHOT
星擊科技股份有限公司 Starshot Tech. Corp.
sales@starshot.tw
(03)610 9677
新竹市東區慈雲路118號17F-1

企業資安風險評等服務

隨著企業面臨大量不同類型的網路威脅，企業除了要掌握本身的安全風險，瞭解委外第三方供應商的安全狀況也成管理重點，星擊科技提供您企業資安風險評等服務(Security Rating Services)，強調可以從企業外部做到網路資安風險分析，並且能基於大數據分析、威脅情報的持續安全監控而成為一種新的資安解決方案。

非侵入性的資訊收集技術

收集公開數據、網路誘捕機制與威脅情資整合

Security Scorecard

指標分析所有安全風險

ThreatMarket
弱點搜索引擎

原廠法律合約
管制不當用途

十組風險因素與易讀的 A–F 評級

網路安全

網路安全模組檢查公共資料集，以查找組織網路內高風險或不安全開放連接埠的證據。

DNS 健康狀況

DNS 運作狀況模組可測量組織的 DNS 設定的運作狀況和配置。它驗證組織網路的被動 DNS 歷史記錄中沒有發生惡意事件。

漏洞修補

漏洞修補模組分析組織安裝安全更新的速度，以衡量脆弱性風險緩解的做法。

端點安全

端點安全模組追蹤從作業系統、網頁瀏覽器和相關的啟用插件所提取的元數據相關的識別點。

惡意 IP 連線信譽評等

網路安全模組檢查公共資料集，以查找組織網路內高風險或不安全開放連接埠的證據。

應用程式安全

應用程式安全模組利用從已知易受攻擊條件獲得的威脅情報，這些條件通過白帽子 CVE 資料庫、黑帽子攻擊資料庫和主要搜索引擎索引的敏感發現進行識別。

Cubit score

Cubit Score 模組評估組織可能存在的各種安全問題。例如，我們會查看公共威脅情報數據庫，以尋找被標記的 IP 地址。

駭客情資

駭客情資模組是用於自動收集和匯總多個地下駭客交流串流的分析系統。

資訊洩漏

資訊洩漏模組利用聊天監控和深網監控功能，以識別駭客傳播的被犯罪的認證資料。

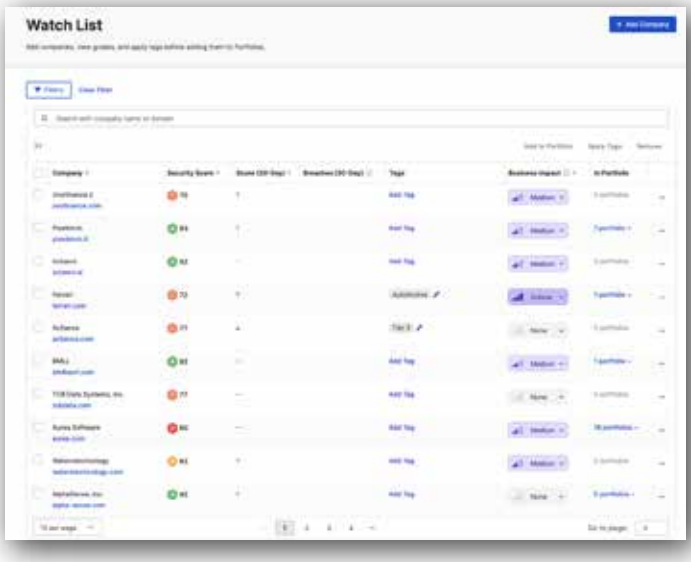
社交平臺分析

社交工程模組用於確定組織對有針對性的社交工程攻擊的易受性。

STARSHOT
星擊科技股份有限公司 Starshot Tech. Corp.
sales@starshot.tw
(03)610 9677
新竹市東區慈雲路118號17F–1

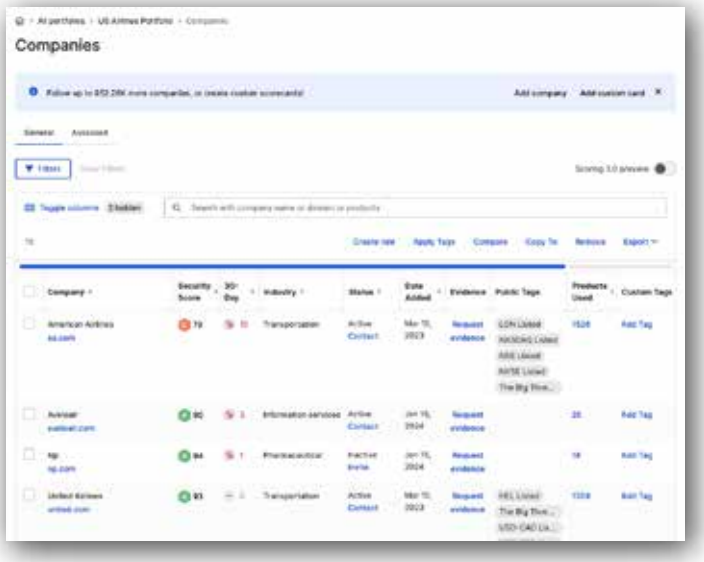
立即了解第三方合作夥伴的網路風險

98% 的組織與至少一個在過去兩年發生漏洞的供應商有聯繫。隨著全球攻擊面不斷擴大，安全和供應商風險管理團隊需要全面了解整個供應鏈。自動化您的第三方風險管理工作流程，發現隱藏的漏洞，並與您的合作夥伴合作建立安全的供應鏈。



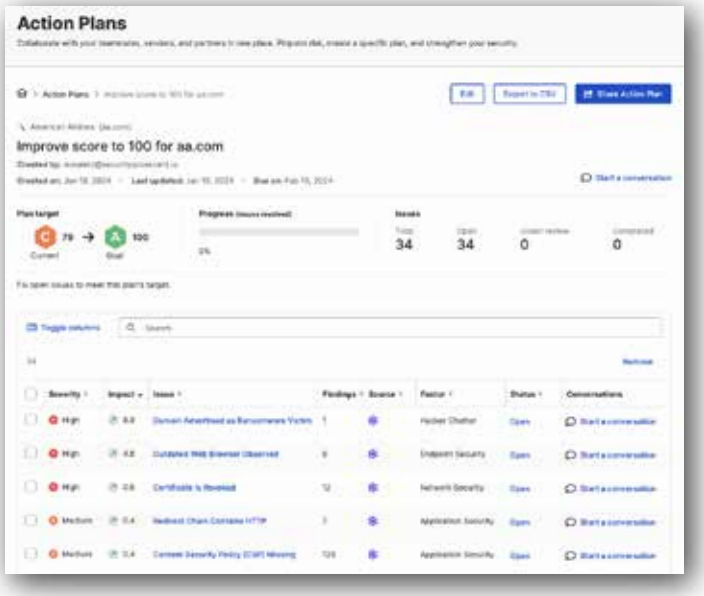
使用短短幾秒評估您的第三方合作夥伴

透過可視化清單（供應商風險評分和業務影響的高級視圖）快速了解生態系統中的潛在威脅



建立投資組合並深入了解細節

輕鬆匯入已知連結，依照重要程度標記與分層，並持續監控數位生態系統中的漏洞與問題



從識別風險到解決風險

邀請您的供應商加入平台，共同制訂行動計畫並進行協作

STARSHOT
星擊科技股份有限公司 Starshot Tech. Corp.
sales@starshot.tw
(03)610 9677
新竹市東區慈雲路118號17F–1

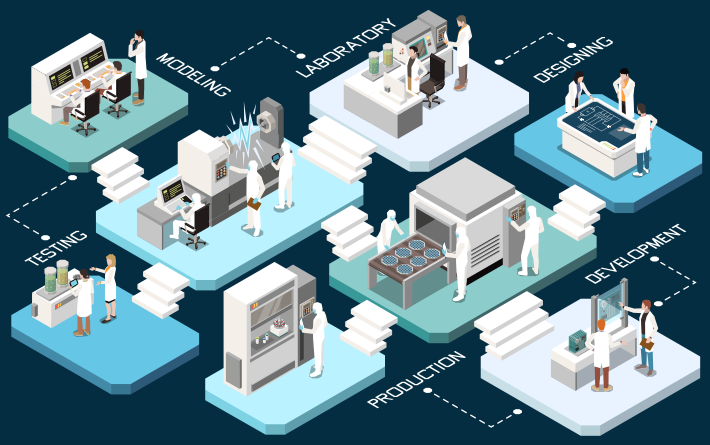
從廠房到企業的工控資安解決方案

隨著連線功能越強大，安全威脅也面臨更大的風險。這些威脅可能有多種形式，從惡作劇駭客到善意的錯誤等。網路資安事件可能會影響網路的可用性、中斷運作及導致生產力中斷。在您面臨安全威脅時，您需要值得信任的專家團隊提供卓越的保護，助您持續創新與發展。我們的工業資安服務可協助保護您的基礎建設、保護資產及維護網路的可用性。

A.I.C

1. 強調可用性
2. 需要較長回覆時間或人工替代
3. 設備系統老舊
4. 不易取代
5. 資安設備少，攻擊面大

OT vs IT



C.I.A

1. 強調機敏性
2. 快速回復能力有HA架構
3. 設備汰換率高系統持續更新
4. 彈性高
5. 資安防護能力高

工業網路安全三階段

我們的方案提供 IT 和 OT 解決方案，涵蓋一連串攻擊事件前、中、後期全程防護。從可改善連線工廠透明度的資產安全評估和連續監視，到威脅偵測及回應和復原的規劃，我們都能全程協助您有效率地保護您基礎結構的安全與運作。

事前	事中	事後
識別與保護	偵測	回復與還原
資產盤點服務	即時威脅偵測服務	備份與復原解決方案
合格修補程式管理	遠端監測與管理服務	
漏洞與風險評估	事件處理與回應	
ICS 安全區域與對策部署	事件回應與災難復原規劃服務	

STARSHOT
星擊科技股份有限公司 Starshot Tech. Corp.
sales@starshot.tw
(03)610 9677
新竹市東區慈雲路118號17F-1

建立更安全的工業控制系統

災難復原

接收
當發現主配置和設備運行版本之間存在差異時收到警報。

備份
自動備份應用程式代碼和設備配置。

最小化
最小化因設備故障而導致的系統停機時間。

確認
確認目前設備中已經正確載入了正確的程式。

生命週期管理

掃描
掃描網路並發現在您的工廠中運行的設備和軟體套裝。

存取
與產品兼容性和下載中心整合，以獲取最新的設備生命周期訊息。

準備
使用產品生命周期數據制定主動的遷移策略。

變更與版本管理

維護
對所有系統資產進行完整的版本控制。

查找
您設備配置或應用程式代碼的最新版本。

查看
使用即時報告查看同一受管理資產的兩個版本之間的差異。

操作員追溯

稽核
即時監控設備配置和應用程式代碼的變更。

查看
查看誰（以及何時）對設備配置和應用程式代碼進行了更改。

遵守
通過詳細的更改稽核軌跡符合監管要求。

系統安全

安全
確保對控制系統的安全存取。

防止
未經授權或不需要的更改對生產產生影響。

檢測
對關鍵過程變量或控制程序的篡改。

通知
利益相關者有關未經授權或不需要的更改。

Continuous Theat Detection 實時監控您的 ICS 網路

網路拓撲

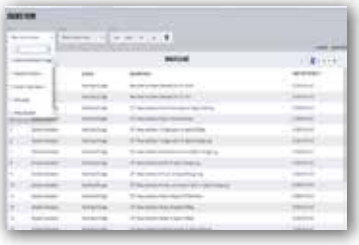
網路拓撲層次化

不僅是顯示完整的網路拓撲架構，更近一步將資產在工控環境的類別分成五個層級顯示

事件偵測

實時偵測整個工控環境

資產變化、行為異常偏差、威脅事件、違反政策等異常事件



資產可視性

廣泛的資產清單

自動識別資產詳細資料，包含 IP、MAC、資產類型、廠牌等資料，可識別的資料協議近 200 種

完整事件分析

提供所有必要的信息以進行分析和修復

完整串聯警報的 IT/OT事故，並將事故發生原因轉化成管理人員可讀的描述，而不是程式碼

基準線自動學習

以基準線進行行為偏差檢測

在正常操作期間自動發現 OT 基準可以檢測偏差和惡意活動

客製化面板

提供有關 OT 網路狀態的信息概覽

客製化面板，可以根據不同角色顯示不同訊息

STARSHOT
星擊科技股份有限公司 Starshot Tech. Corp.
sales@starshot.tw
(03)610 9677
新竹市東區慈雲路118號17F-1

勒索檔案解密服務

星擊為您提供的勒索檔案解密服務不僅限於提供技術上的支援，更強調客戶的整體安全。我們的專家團隊將與您合作，制定預防勒索攻擊的有效措施，包括提供安全複製建議、強化防病毒措施以及執行定期安全檢查。

面對駭客勒索，您的企業準備好了嗎？

STAGE 1	STAGE 2	STAGE 3	STAGE 4
協助客戶做 IP 調查	資料被加密，急需救回重要資料	資料若無法順利解密或只能部份解密	資安事件後做企業資安整體評估服務
了解受駭範圍並協助清除	協助評估可還原性及解密	協助客戶與駭客談判	避免事件再次發生

加快業務成長

創新可以幫助您在生命週期的每個階段以更快、更聰明和更敏捷的方式工作

改善生產力

透過資料分析而下的決策，持續提高績效和產量

締造員工績效

安全地連接人員、流程和技術

驅動永續性

採行兼具環保和經濟的製程

管理風險

在保護人員和流程的同時，遵循適法性和品質標準

STARSHOT
星擊科技股份有限公司 Starshot Tech. Corp.
sales@starshot.tw
(03)610 9677
新竹市東區慈雲路118號17F-1

STARSHOT

Your best system integration consulting partner.

STARSHOT
星擎科技股份有限公司 Starshot Tech. Corp.

sales@starshot.tw
(03)610 9677
新竹市東區慈雲路118號17F-1