感謝您參與今天活動，您可以掃描畫面上QR Code參加我們的小遊戲

2025台灣二版

資安講堂-NordStellar

攻擊面管理：從外部資產到威脅預測

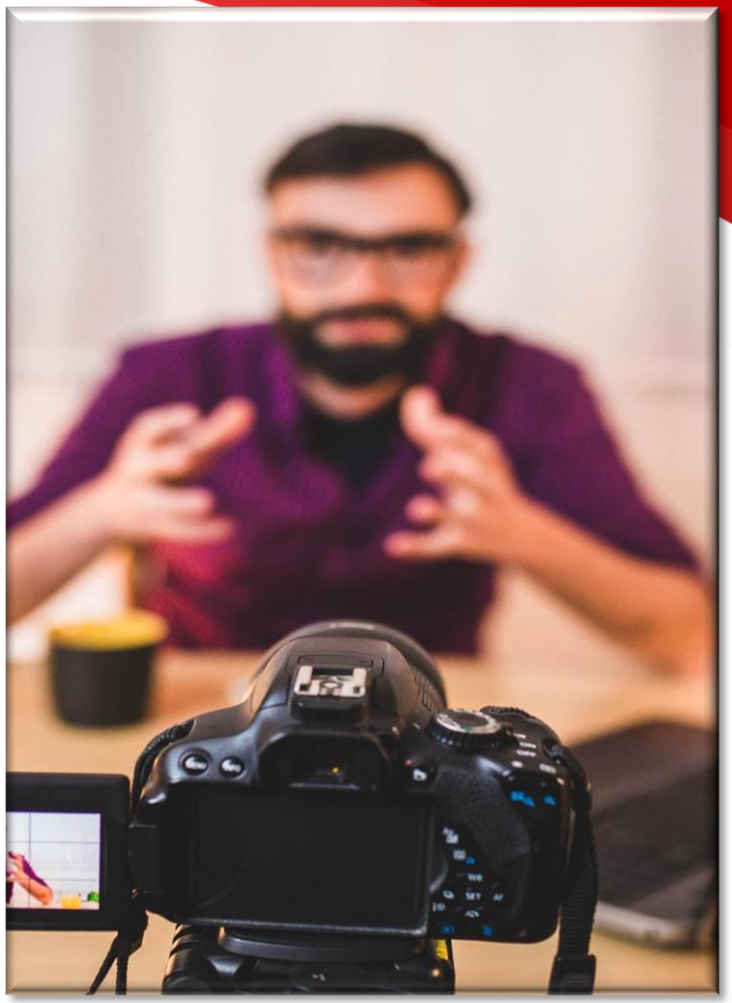
NordStellar 產品介紹

Version 2 台灣二版

- 主講人：

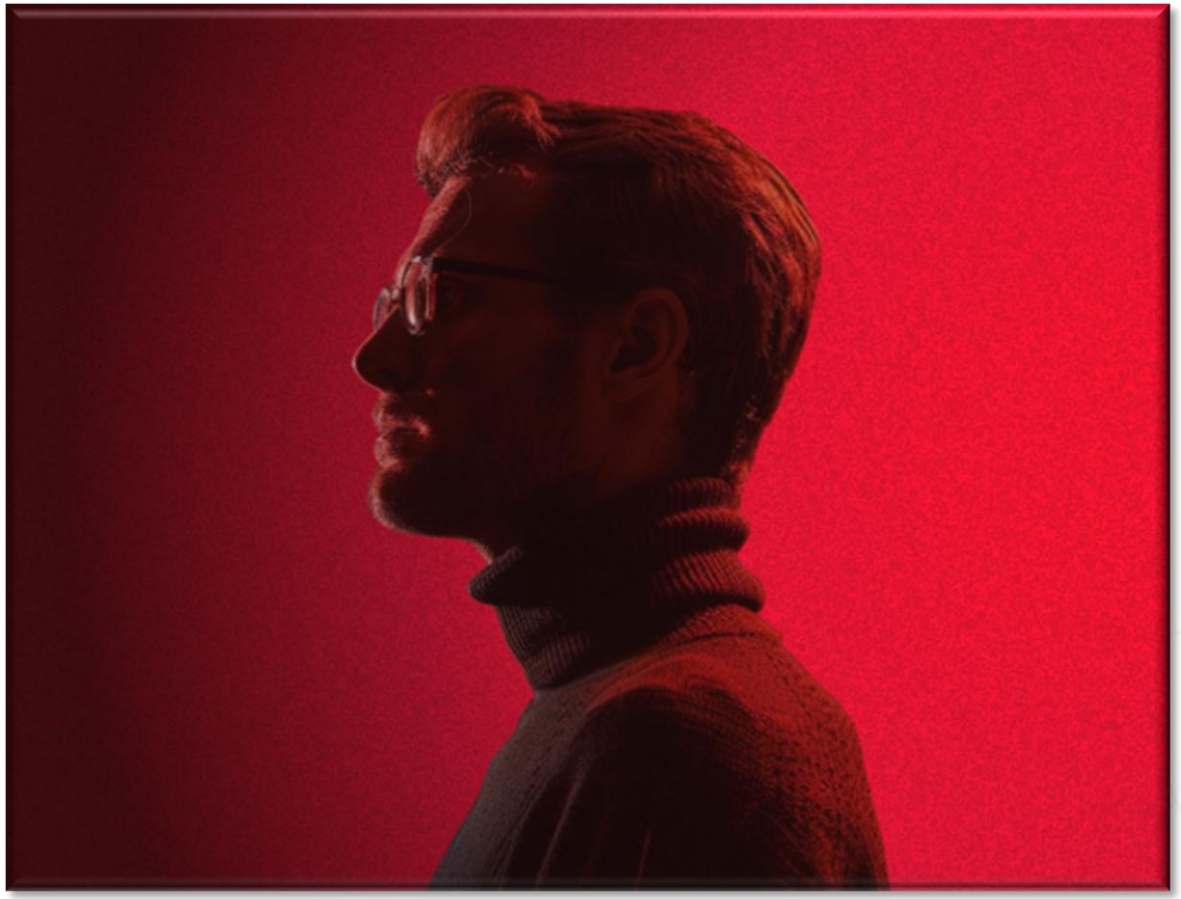
議程內容

- NordStellar產品背景
- NordStellar解決方案
- NordStellar保護功能
- Q&A



Nord產品背景

關於Nord Security



我們的故事始於 Nord Security，也就是 NordVPN 背後的公司。在那裡，我們的網路安全團隊面臨著令安全主管們夜不能寐的同樣挑戰。

作為一家網路安全公司，我們的目標是發現並應對可能。我們深知您面臨的挑戰—因為我們也曾經經**導致財務和聲譽損失的威脅**歷過。我們曾處理過大量的威脅數據，試圖從中理清頭緒。那段經歷令人不堪重負，我們知道一定有更好的方法。

NordStellar 不僅僅是一款工具，更是我們分享知識和經驗的方式。我們**監控數千個網路犯罪社群、深網和暗網網站**，確保網路安全團隊擁有正確的資訊和工具，以便做出更明智的決策。

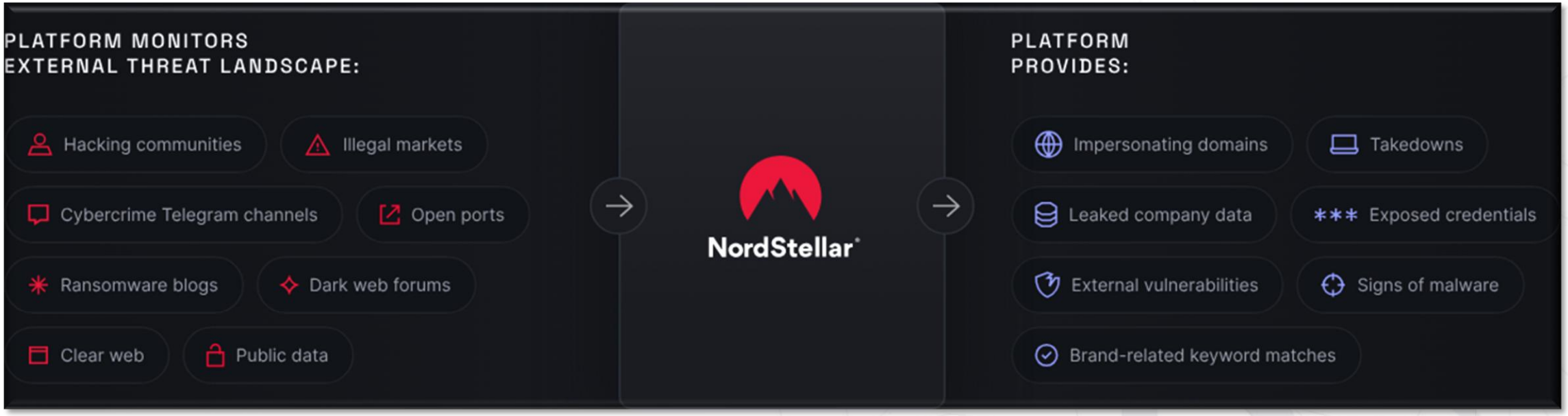
20,000+
使用 Nord Security 產品保護的企業

10+
上市多年

2,000+
全球員工

NordStellar優勢

網路犯罪分子依靠隱蔽性和突襲，在您最意想不到的時間和地點發動攻擊。 NordStellar 讓您重新掌控局面，讓您能夠洞察隱藏的威脅，從而在它們影響您的業務之前採取行動。



800B+
拯救資產

90B+
洩漏的憑證

50M+
分析惡意軟體攻擊

40K+
監控來源

NordStellar優勢(續)

- 風險排序、將集中注意力在最重要事件(降噪)。
- 定期/持續地從外部角度掃描。
- 大量暗網與外部情資的資料。
- 介面友善。
- 減少直接逛暗網論壇時遇到下載檔案內夾帶惡意檔案、假資料等。
- 自寫爬蟲造成反制或被鎖定攻擊的目標。

為什麼選擇NordStellar

大量數據

利用超過 **36,000** 個接觸點的關鍵威脅洞察，包括暗網駭客論壇、勒索軟體部落格和 Telegram 頻道。

即時監控和警報

一旦偵測到您的**業務資料洩露**，您將立即收到通知，以便在攻擊者採取行動之前採取措施。

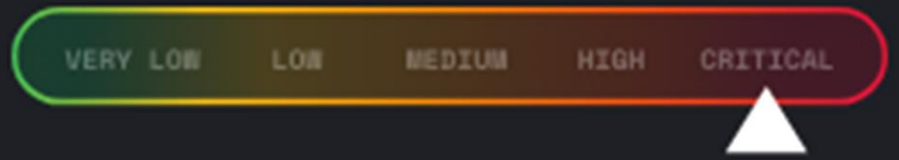
基於風險的優先排序

根據**業務影響、洩漏機率和真實攻擊者行為對風險敞口**進行排序，從而集中精力應對最大的威脅。

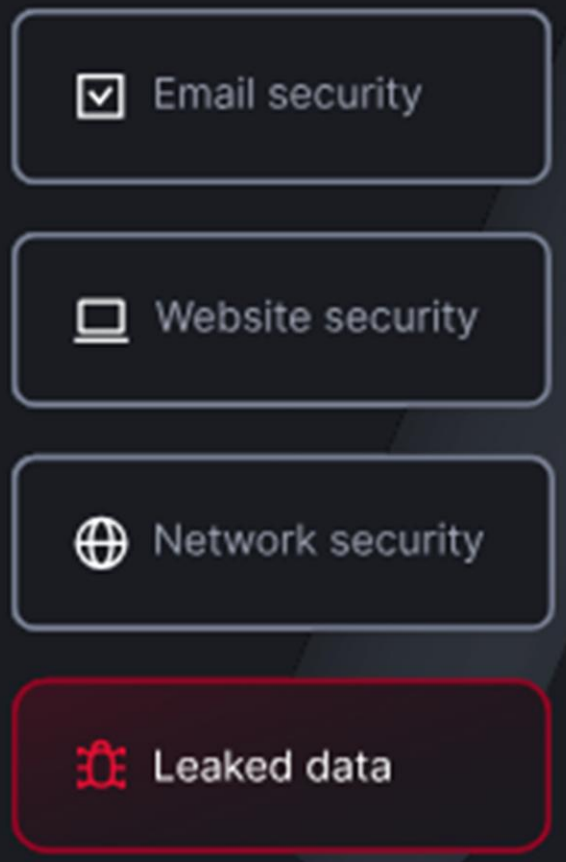
一個集中式平台

透過將您的**安全漏洞、暗網和攻擊面情報整合到一個平台**，減少技術債並增強控制力。

敏感資料外洩重要性



- 了解攻擊者對貴公司所掌握的信息，並在資產成為攻擊目標之前識別出這些暴露的資產。
- 評估資料外洩、網路安全、網路應用程式安全和電子郵件安全風險。
- 幫助高階主管了解安全漏洞及其潛在影響。



在保持安全和掌控做了什麼?

資料外洩監控

透過即時監控和警報，識別並減輕員工和消費者資料外洩（包括憑證外洩或被盜）所帶來的風險。

品牌保護

透過偵測、移除和阻止未經授權的線上品牌使用行為，防止欺詐，維護您的聲譽和客戶信任。

暗網監控

在暗網論壇、網路犯罪社群和 Telegram 頻道中追蹤與公司相關的關鍵字，以便領先於針對您企業的威脅。

攻擊面管理

利用自動化資產發現功能繪製您的基礎架構（Web 伺服器、應用程式、網域等），並結合即時外部威脅偵測，以彌補安全漏洞。

NordStellar解決方案

資料外洩監控

- 在員工和消費者資料遭到利用之前，偵測並清除已洩漏的資料。
- 監控來自多個來源的惡意軟體和資料外洩事件。
- 最大程度降低勒索軟體和帳戶盜用帶來的風險。

什麼是資料外洩監控？

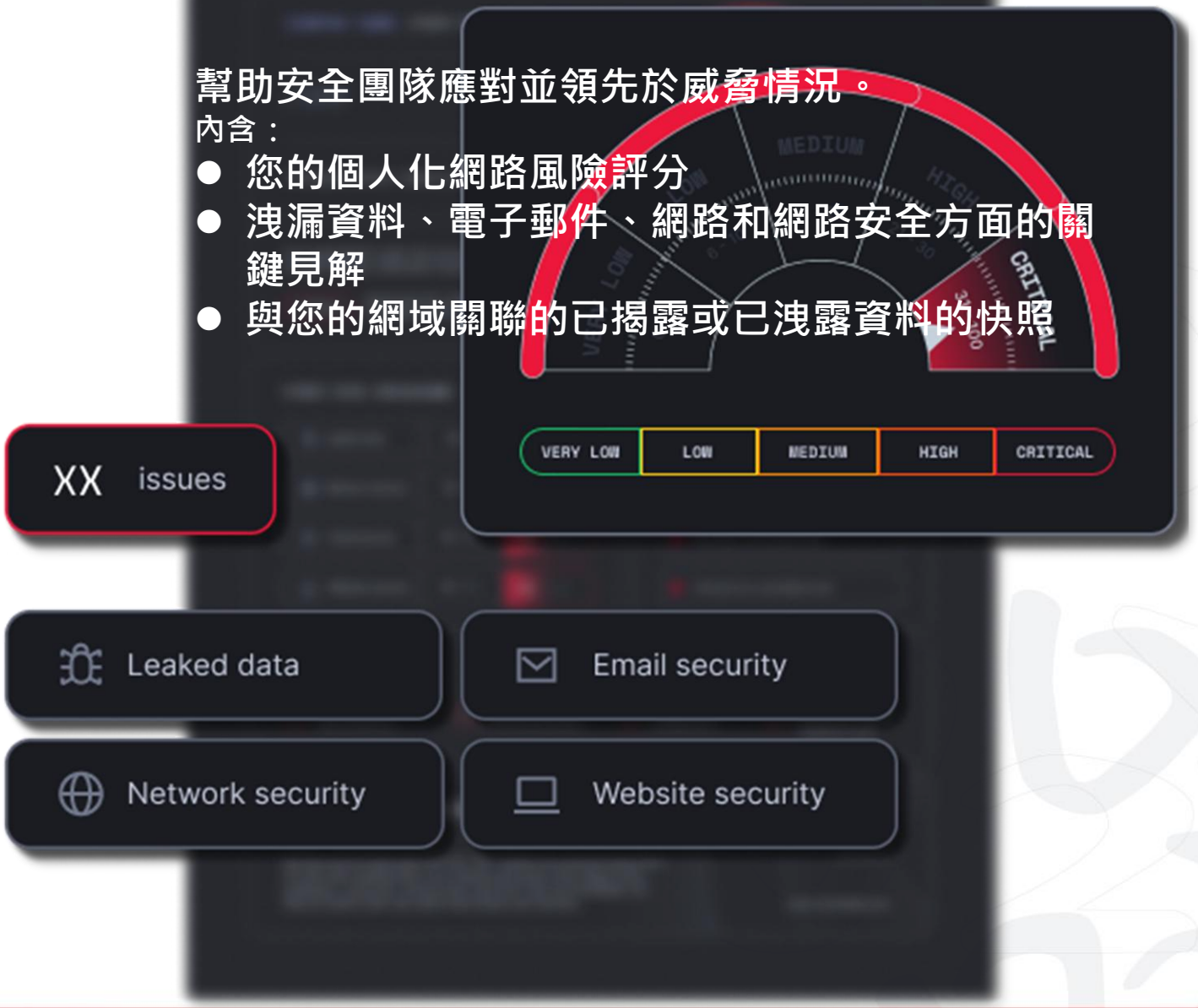
資料外洩監控是指持續掃描深網、暗網以及其他來源（例如 Telegram 頻道）的過程。它有助於檢測各種類型的洩漏數據，例如憑證、電子郵件、信用卡號、社會安全號碼和其他個人識別資訊 (PII)。資料外洩檢查有助於公司及時控制威脅並防止進一步損害。

公司資料安全狀況

幫助安全團隊應對並領先於威脅情況。

內含：

- 您的個人化網路風險評分
- 洩漏資料、電子郵件、網路和網路安全方面的關鍵見解
- 與您的網域關聯的已揭露或已洩露資料的快照



資料外洩工作原理

資料收集

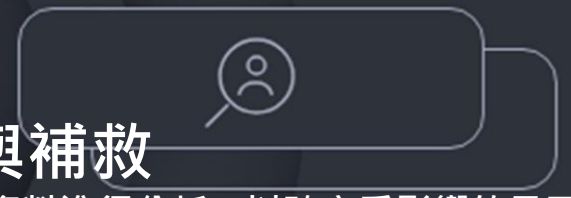
資料收集自各種來源，例如深網和暗網、Telegram 頻道、勒索軟體部落格和威脅行為者社群。

監控和警報

持續監控會在員工或消費者資料外洩時向公司發出警報。

強化蒐集資料

新增相關上下文信息，例如洩漏源、日期和受影響的資料點，以豐富收集到的資料。



分析與補救

對洩漏的資料進行分析，以確定受影響的員工和消費者，並做出適當的回應。

偵測出資料外洩事件

一個密碼外洩就可能為公司帶來嚴重問題。您可能會面臨嚴重的網路安全事件、消費者資料洩露，以及因聲譽受損和監管罰款而造成的巨額經濟損失。但NordStellar的資料外洩監控服務可以幫助您避免這些損失。

資料外洩監控可協助您偵測員工和消費者資料外洩狀況，並在網路犯罪者利用惡意軟體之前識別感染惡意軟體的公司設備。

可能外洩漏資訊有哪些?

個人識別資訊（PII）

姓名、家庭住址、電話號碼、出生日期、社會安全號碼和政府核發的身份證件

財務資訊

信用卡詳細資料、銀行帳號、交易記錄和帳單地址。

登入憑證

使用者名稱、密碼、令牌、安全性問題和活動會話 cookie。

醫療記錄

病患健康資料、保險詳情和處方記錄。

企業數據

商業機密、商業策略、客戶資訊和智慧財產權。

員工數據

薪資數據、稅務資訊和內部溝通記錄。

消費者數據

電子郵件地址、購買歷史記錄和支援互動記錄。

資料外洩監控帶來的好處

全面覆蓋

資料外洩偵測工具提供洩漏偵測、威脅警報、存取業界最大的深網和暗網資料池之一，以及全面的報告，以幫助您預防各種風險。

風險評估和優先排序

評估每次違規的嚴重程度，並幫助您的團隊首先集中精力處理最緊迫的風險。

即時警報

持續監控有助於在網路犯罪分子利用漏洞之前發現它們。及早收到洩漏憑證的警報並採取行動。

易於集成

該軟體易於整合到現有安全系統中。

資料外洩常見問題

● 什麼才算資料外洩？

資料外洩是指任何未經授權的第三方取得私人、敏感或機密資訊的安全事件。資料外洩的類型包括憑證外洩、財務資料竊取和個人資訊外洩。

● 資料外洩有多嚴重？

資料外洩是一個非常嚴重的安全問題，往往會**導致法律處罰、消費者信任度下降和經濟損失**。如果沒有資料外洩監控系統，評估損失的真實範圍可能會很困難。

● 資料外洩最常見的原因有哪些？

資料外洩可能由多種原因造成。例如，弱密碼很容易被猜到，或在網路釣魚攻擊中被洩露。網路釣魚攻擊也可能導致敏感資料外洩。其他原因還包括惡意軟體、未修補的軟體漏洞、人為錯誤、第三方供應商漏洞以及安全設定錯誤。

● 資料外洩事件需要多久才能恢復？

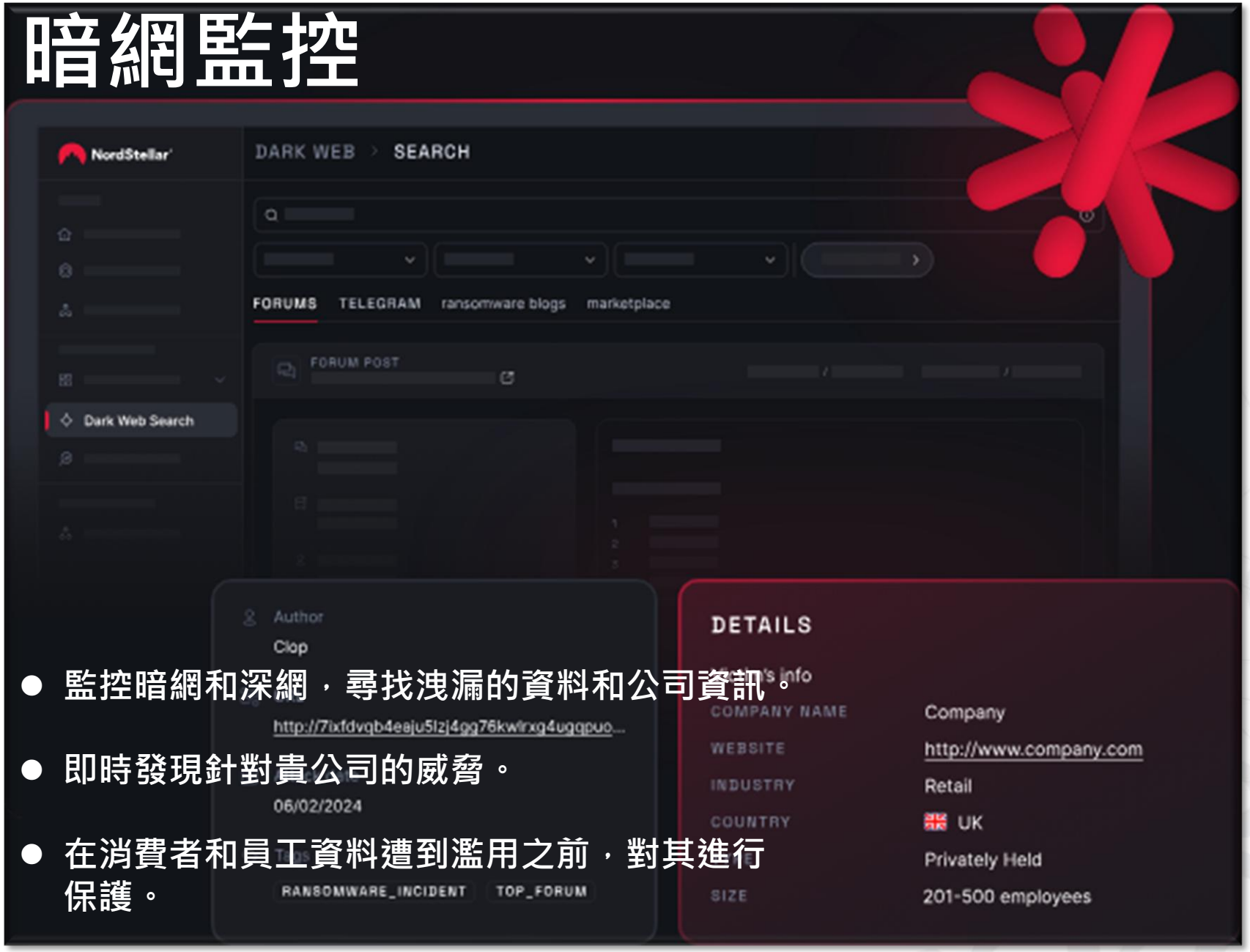
從任何網路安全事件（例如資料外洩）中恢復所需的時間取決於事件的嚴重程度。據 IBM 稱，通常需要大約 **204 天**才能識別出資料外洩事件，還需要額外 **73 天**才能控制住。如果憑證被盜，所需時間通常會更長。

● 資料外洩後應該立即採取哪些措施？

如果貴公司遭遇資料洩露，迅速採取行動並控制洩漏範圍必須是首要任務。這意味著隔離受影響的系統、停用被盜帳戶並限制未經授權的存取。之後，您需要評估情況並採取措施防止未來再次發生類似事件：

1. 評估損失。
2. 通知相關利害關係人。
3. 調查並記錄此違規事件。
4. 加強安保措施。
5. 向有關部門報告。
6. 利用資料外洩監控持續檢查資料外洩。

暗網監控



- 監控暗網和深網，尋找洩漏的資料和公司資訊。
- 即時發現針對貴公司的威脅。
- 在消費者和員工資料遭到濫用之前，對其進行保護。

暗網監控工作原理

NordStellar的暗網監控服務為企業提供被竊或外洩資料的即時可見性。透過持續掃描暗網，它可以幫助您及早發現資料外洩事件並預防潛在威脅。

● 持續暗網監控

NordStellar持續掃描暗網和深網資源——從隱藏論壇到Telegram頻道和勒索軟體部落格——並在**新洩漏資訊出現的第一時間將其檢測到**。與單一快照不同，持續監控讓您隨時掌握新出現的風險。

● 持續的資產和關鍵字監控

監控數千個來源中提及貴公司、員工或合作夥伴的資訊。**從網域和電子郵件到特定關鍵字或供應商**，NordStellar 透過一次性搜尋和持續跟踪，幫助您識別潛在風險。

● 透過您的通訊工具接收即時提醒

一旦偵測到新的威脅，您將**立即收到通知——直接透過電子郵件、Slack、Microsoft Teams 或其他您偏好的管道接收**。自動警報確保您的安全團隊能夠在事件擴大之前做出回應。

● 視野開闊，解析度更高

檢測到的每次提及都帶有豐富的**上下文資訊**——包括連結、作者和來源詳情，有時甚至還有螢幕截圖——因此您可以自信地採取行動。

監控的威脅來源

暗網論壇

NordStellar 擁有**多年監控深網和暗網的經驗**，可以存取最大的資料池之一，偵測數千個暗網論壇中出現的新威脅。

Telegram頻道

NordStellar 主動**監控數萬個用於詐騙、網路釣魚和身分盜竊的網路犯罪 Telegram 頻道**，快速偵測威脅並預防潛在事件。

暗網市場

NordStellar密切**監控各大暗網市場**。儘早發現貴公司外洩的資訊和敏感資料是否正在非法出售。

勒索軟體博客

我們追蹤數百個勒索軟體博客，以幫助**評估勒索軟體和資料外洩的威脅**。識別您的組織遭受勒索軟體攻擊的風險，並預防這些破壞性極強的攻擊。

暗網監控常見問題

● 什麼是暗網監控？

暗網監控解決方案能夠持續掃描論壇、市場和勒索軟體部落格等隱藏來源，尋找洩漏的公司數據，例如**憑證或網域提及**。 NordStellar 會在敏感資訊出現的第一時間發出警報，幫助您的團隊快速回應，預防潛在的網路安全事件。

● 使用暗網監控來保護我的企業資料安全嗎？

是的。暗網監控完全安全，因為它不會洩漏或共享您公司的敏感資料。 NordStellar **監控外部來源（例如暗網論壇、市場和勒索軟體部落格），並將其與已知的識別碼（例如網域名稱或電子郵件地址）進行匹配**，而無需存取您的內部系統。

● 與一次性掃描相比，暗網監控有哪些優勢？

一次性掃描可以讓你快速了解當前的風險敞口，但持續監控暗網才能確保你隨時掌握最新動態，因為每天都會出現新的洩漏資訊和提及。在**新風險出現的第一時間發出警報**，可以幫助你在威脅造成實際損害之前做出應對。

● 如果暗網監控偵測到洩漏的憑證或數據，我的企業應該採取哪些措施？

如果 NordStellar 偵測到資料洩露，您的安全團隊應立即**重設所有外洩的密碼，調查潛在的安全漏洞，並審查存取控制**。該平台提供完整的上下文資訊（包括來源連結和時間戳），以幫助快速驗證和控制資料外洩。

● 你的暗網掃描器和暗網監視器有什麼不同？

這款免費的暗網掃描器是一款便捷的線上工具，可讓您查看與公司郵箱關聯的洩漏資料範例。 NordStellar 的**全方位暗網監控解決方案提供對數千個來源的持續自動掃描、即時警報和詳細情報**，從而實現持續保護。

暗網監控常見問題(續)

- **使用NordStellar暗網掃描安全嗎？**

是的，免費掃描完全安全。它只會將您的工作郵箱與現有的洩漏資料庫進行比對，**不會收集、共享或儲存除顯示結果所需資訊之外的任何敏感資訊**。

- **暗網掃描器掃描後會儲存我的電子郵件或其他資訊嗎？**

不。**您的郵箱僅用於執行掃描並產生報告**。 NordStellar 在結果顯示後不會儲存或重複使用您的資訊。

- **免費暗網掃描報告中會顯示哪些資訊？**

您將看到一份摘要，其中**列出了貴公司電子郵件是否出現在已知的洩漏事件中，以及洩漏的資料類型範例**。報告預覽了 NordStellar 完整的暗網監控平台所提供的洞察功能。

品牌保護

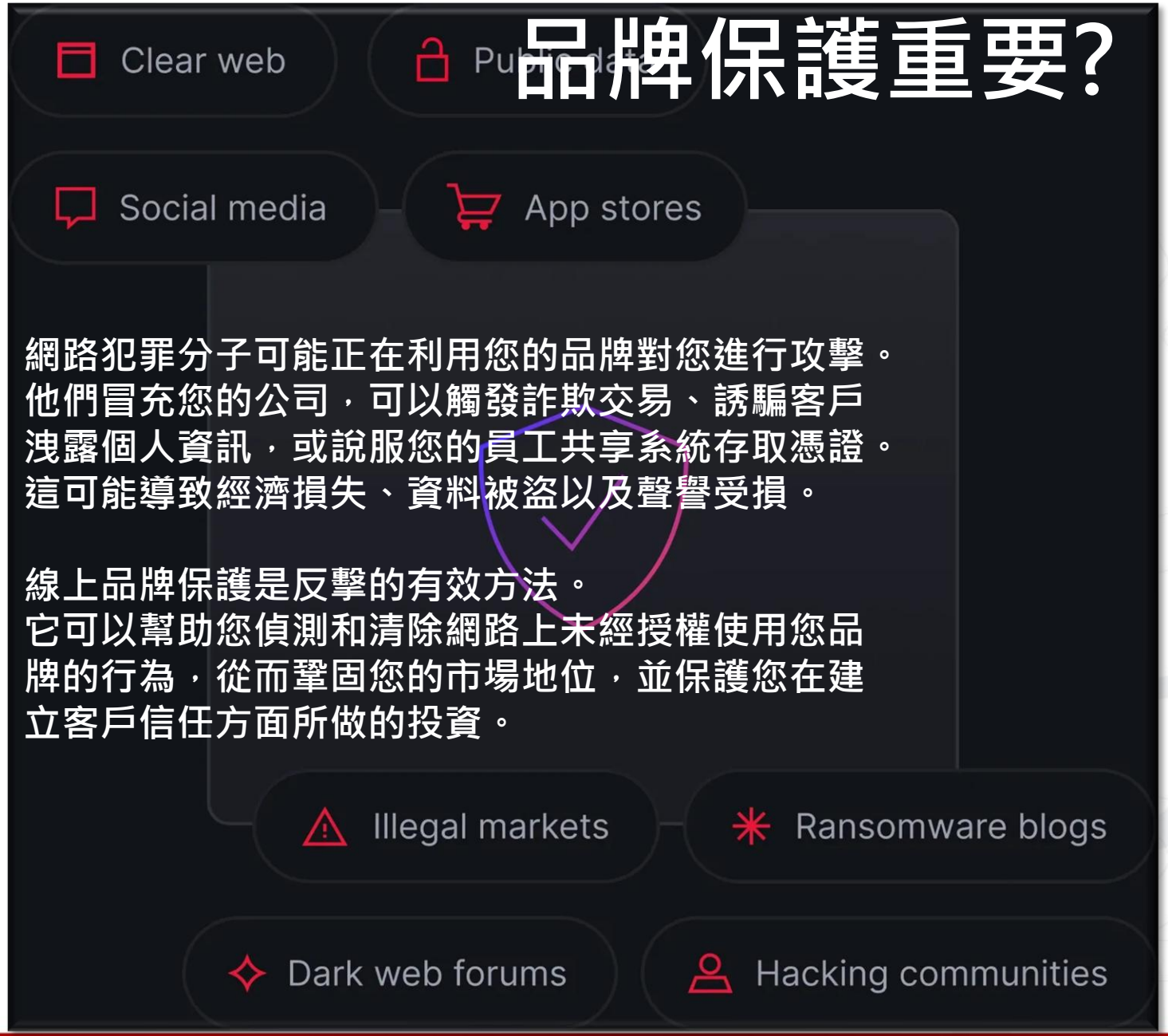
- 輕鬆偵測網路、社群媒體和應用程式商店中的品牌濫用行為。
- 在虛假內容和網站傳播之前迅速將其清除。
- 維護您的聲譽，保持客戶信任。

什麼是品牌保護？

品牌保護是網路安全的關鍵部分，它涉及監控各種線上管道——從網站和社交媒體平台到應用程式商店——以發現未經授權使用品牌資產和其他濫用品牌的跡象。

當檢測到這些違規行為時，線上品牌保護服務可以幫助刪除侵權內容，防止未來濫用行為，從而保護公司聲譽並贏得客戶的信任。

品牌保護重要?



網路犯罪分子可能正在利用您的品牌對您進行攻擊。他們冒充您的公司，可以觸發詐欺交易、誘騙客戶洩露個人資訊，或說服您的員工共享系統存取憑證。這可能導致經濟損失、資料被盜以及聲譽受損。

線上品牌保護是反擊的有效方法。
它可以幫助您偵測和清除網路上未經授權使用您品牌的行為，從而鞏固您的市場地位，並保護您在建立客戶信任方面所做的投資。

優勢在哪裡?

主動防禦品牌冒用行為

監控網路、社群媒體和應用程式商店，以便在**冒充行為損害您的業務之前**發現並阻止它們。

全面打擊支持

在惡意網域、虛假個人資料和詐欺性應用程式**造成更大危害之前**，迅速將其清除。

客戶保護

立即採取行動，制止網路釣魚、詐欺和冒充行為，這些行為會危及您的客戶。

品牌信任維護

防止攻擊者**利用您的品牌名稱、商標和行銷素材欺騙客戶**。

減輕團隊的工作量

實現品牌保護監控和執行的**自動化**以便您的安全團隊專注於創造業務價值的活動。

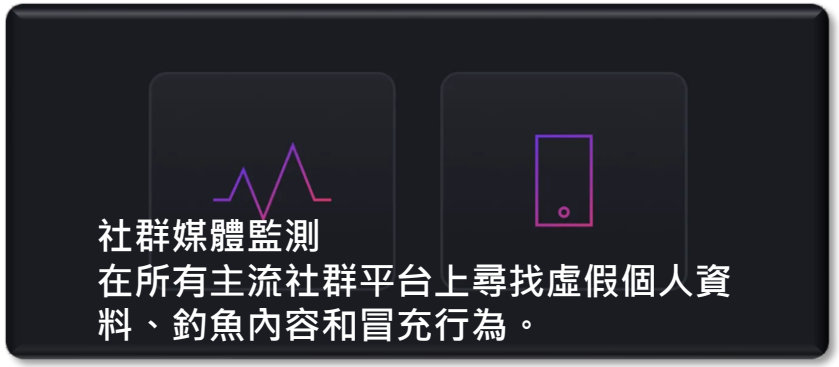
清晰、可操作的見解

取得每月報告，以了解為保護您的品牌而偵測到、解決和移除的內容。

USE CASES

網域名稱和網站保護
識別針對您品牌的相似網域、網域搶註和釣魚網站。

應用程式商店監控
掃描數百個全球應用程式商店，尋找冒充您品牌的克隆或惡意應用程式。



社群媒體監測
在所有主流社群平台上尋找虛假個人資料、釣魚內容和冒充行為。

下架服務
刪除惡意網域、虛假社交帳號和詐欺性應用程序，同時處理自訂下架請求。

品牌保護運作

1

監視器

它會**持續監控網路、社群媒體和應用程式商店**，追蹤您品牌的所有使用情況。

2

分析

它會審查與您的品牌相關的數據，以**識別任何異常、可疑或來自未經授權來源的內容**。

3

消除

它會**自動啟動對偵測到的虛假網站、社群媒體詐騙、應用程式商店盜版應用程式和其他形式的品牌濫用行為的下架程式**。

4

通知

每個月，您都會收到效能報告，其中包含所有已偵測到、已解決和已移除的威脅的完整摘要。

品牌保護常見問題

● 企業若缺乏品牌保護，將面臨哪些風險？

如果沒有品牌保護，企業就有可能失去其獨特的品牌標識，被造假者或仿冒者竊取，這會**嚴重削弱品牌價值，讓消費者感到困惑**。這會導致消費者信任度下降，尤其是在假冒產品或詐騙行為損害品牌聲譽的情況下。更糟的是，企業還可能捲入棘手的法律糾紛，耗費大量時間和資源來解決。

● 品牌保護能否幫助公司抵禦資料外洩？

品牌保護在抵禦資料外洩方面發揮輔助作用，它有助於**保護您的智慧財產權、商標和聲譽免受濫用和仿冒**。其中關鍵的一環是監控品牌冒充行為，例如虛假網站或網路釣魚詐騙，這些行為往往被用作網路攻擊的入口。透過及早發現這些威脅，品牌保護可以幫助防止其升級為全面的資料外洩事件。

● 品牌保護如何為威脅情報做出貢獻？

品牌保護透過監控和識別與公司品牌相關的風險（涵蓋社群媒體平台和應用程式商店等公共攻擊面），為威脅情報做出貢獻。這種更廣泛的可見性有助於發現那些可能被忽視的威脅，為公司提供寶貴的洞察，從而主動捍衛其聲譽和資產。

● NordStellar能否協助偵測暗網上的品牌濫用行為？

是的，NordStellar **可以協助偵測暗網上的品牌濫用行為，進而保障品牌安全**。其暗網監控解決方案會持續掃描暗網論壇、非法市場、深網資源、Telegram 頻道和勒索軟體博客，查找與品牌相關的關鍵字和提及。這樣，您就可以在假冒產品、詐欺網域或冒充者造成重大威脅之前，及時發現並解決這些問題。

● 品牌保護是否有助於遵守監理規定？

是的，**品牌保護有助於企業遵守監管規定，確保公司的商標、產品標籤和行銷材料符合法律標準和行業法規**。它還有助於防止假冒或未經授權的產品流入市場，這些產品可能造成安全或品質風險，並導致監管處罰。此外，網域品牌保護在阻止可能導致合規問題的詐騙網站或網域搶注網站方面也發揮著至關重要的作用。

攻擊面管理

更了解公司的攻擊面。

尋找並修復外部數位資產中的漏洞。

請確保您符合必要的合規要求。

什麼是攻擊面管理？

攻擊面管理 (ASM) 是指管理所有連網資產，以識別和預防潛在風險的過程。透過監控外部資產的暴露情況，它可以幫助您的公司在漏洞被利用之前將其解決。透過 NordStellar，您可以輕鬆發現系統中的弱點並預防多種網路威脅。

攻擊面管理運作

1

鑑別

為了幫助您收集信息，NordStellar 實現了**自動資產發現功能。它利用 DNS 枚舉、網路爬蟲和其他開源情報 (OSINT) 技術等多種手段**，識別與組織相關的所有暴露在網路上的資產。

2

分析

NordStellar 可協助您**分析資產中的潛在漏洞**。例如，它使用被動服務指紋識別技術掃描已發現的資產，尋找已知漏洞。

3

評估

NordStellar 透過根據**威脅的嚴重性、可利用性和潛在影響對其進行優先排序和評估**，幫助您更好地了解各種威脅。

4

補救措施

這一階段的重點在於**彌補安全漏洞**。例如，NordStellar 提供即時警報和全面報告，涵蓋組織面臨的新漏洞和攻擊面變化。

攻擊面管理可以偵測到那些問題?

- **子域名**

未被監控或遺忘的子網域可能成為攻擊者的入口點。

- **暴露的服務**

面向互聯網的服務，例如資料庫或檔案共享系統，可能會**無意中允許未經授權的存取**。

- **暴露的 IP 位址**

未加密或已被遺忘的IP位址，可能成為攻擊者的目標。

- **未修復的漏洞**

存在**已知漏洞、亟需修補**的過時軟體。

- **雲端服務配置錯誤**

配置不當的雲端伺服器會洩漏敏感資料。

- **影子IT資產**

未經IT部門批准，員工使用**未經授權的應用程式或系統**。

- **第三方風險**

供應商或合作夥伴**有權存取您的系統或數據**，由此產生的風險。

攻擊面管理優勢

攻擊面管理的主要優勢在於識別弱點並系統性地降低風險。一旦找到並消除不必要的資產，就可以根據威脅的嚴重程度或對公司的潛在影響來確定其優先順序。

但NordStellar的功能遠不止於此。它不僅能幫助您識別漏洞並主動解決安全隱患，還能透過自動化ASM任務，幫助您節省成本、滿足監管要求並提高營運效率。

攻擊面管理常見問題

● 什麼是攻擊面？

攻擊面是指**系統中所有可被利用的入口點總數**。入口點包括硬體、軟體和雲端基礎設施，但也應考慮人為錯誤和物理社會工程攻擊手段。

● 為什麼攻擊面管理如此重要？

攻擊面管理 (ASM) 可**協助您了解自身漏洞，並在網路犯罪分子利用這些漏洞之前將其堵住**。組織的攻擊面可能非常廣泛，包括遺留資產、供應鏈中的安全漏洞以及業界普遍存在的漏洞。 ASM 可協助您發現未知風險，並保護您的組織、合作夥伴和客戶。

● NordStellar是如何發現我的外部攻擊面的？

NordStellar 利用其**專有的網域枚舉技術來發現您外部攻擊面的弱點**。例如，掃描公共網站和暗網可以幫助它發現駭客論壇中提及您企業的線索，並識別潛在的安全漏洞。

● NordStellar可以偵測到哪些類型的安全性問題？

NordStellar可以偵測多種類型的安全性問題：

1. 開放埠
2. 暴露的服務
3. 配置錯誤的服務
4. 過時的軟體
5. 不支援的設備
6. 影子基礎設施

攻擊面管理常見問題(續)

● ASM能否在合規方面提供協助？

遵守 GDPR 和 HIPAA 等隱私權法律法規通常取決於正確的資料儲存和保護流程。 ASM 旨在彌補您安全方面的漏洞，因此可以極大地幫助您**遵守區域隱私法律以及 ISO 27001、NIS2 和 DORA 等全球標準和法規**。

● 如何選擇最佳的攻擊面管理解決方案？

選擇最佳攻擊面管理解決方案的關鍵在於評估貴公司的特定需求。需要考慮**基礎設施的規模、資料的敏感度以及外部資產的複雜性**。

歸根結底，攻擊面監控是一個持續的過程，因此找到一家信譽良好的公司並與之長期合作至關重要。 NordStellar 就是這樣一家公司。作為Nord Security的一部分，NordStellar 提供多年的網路安全專業知識、用於主動威脅偵測的現代化工具以及進階攻擊面監控。

NordStellar保護功能

帳號盜用預防

即時識別被盜帳戶。
防止針對高階主管帳戶的定向存取。
避免聲譽受損和經濟損失。

什麼是帳戶盜用？

帳戶盜用（ATO）是一種網路攻擊，網路犯罪分子利用竊取的憑證非法存取企業系統。犯罪者通常從暗網或Telegram等平台免費取得使用者憑證，他們也可能大量購買或透過網路釣魚攻擊來取得這些憑證。

一旦控制了帳戶，攻擊者就可以利用被入侵的帳戶進行惡意活動，例如竊取公司資料、提取資金，甚至利用公司帳戶進行詐騙活動。

如何防止帳號盜用?

● 早期檢測

及早發現威脅始於對企業帳戶的監控。個人資訊變更、可疑交易以及惡意軟體感染、資料外洩等網路安全事件，都可能預示著帳戶遭受了劫持攻擊。主動監控帳戶有助於您快速找到應對新出現的威脅的最佳方法。

● 教育

教育和安全培訓至關重要，因為了解需要注意的事項能更容易識別潛在威脅。盡可能對員工進行反盜用攻擊（ATO）的教育，並安排訓練課程，幫助他們辨識社會工程攻擊手段。

● 良好的網路安全習慣

在數位化世界中，密碼安全至關重要。公司應**強制推行使用強密碼和唯一密碼的政策，或採用企業密碼管理器集中管理密碼**。確保所有公司帳戶都啟用身份驗證方法，例如金鑰驗證和多因素身份驗證(MFA)，並遵循 NIST 框架建立完善的網路安全實踐。

● 帳戶被盜保護解決方案

使用帳戶盜用防範解決方案（例如 NordStellar）可以**集中管理您的帳戶安全**。帳戶盜用防範解決方案可協助您監控可疑活動、偵測未經授權的存取嘗試，並提供即時警報。

防止帳號盜用機制運作

主動用戶掃描
NordStellar 將您組織現有的帳戶與從 Telegram、深網和暗網重新取得的資料交叉比對。

密碼模糊測試
NordStellar 可即時偵測暴露的憑證和活動的會話 cookie，協助您避免帳戶被盜用。

防止憑證外洩和濫用
NordStellar持續監控使用者登入表單域名，以深入了解被盜憑證的使用情況。

帳號盜用防護重要性

潛在的經濟損失

未能發現帳戶盜用威脅可能導致**因詐欺、監管罰款和法律責任而造成的重大經濟損失**。

不遵守資料隱私法規可能會導致巨額罰款，而詐欺交易和未經授權的存取可能會對您的企業造成直接的財務損失。

人為錯誤是不可避免的

軟體漏洞和人為錯誤對資料外洩、系統故障和帳戶盜用都起著同等重要的作用。

雖然可以透過培訓和集中式帳戶管理來減少人為錯誤，但**不良的密碼習慣、惡意軟體或複雜的社會工程手段**仍然會帶來持續的安全威脅。

名譽損害

帳戶被盜不僅會影響公司財務狀況，還會嚴重打擊客戶信任。
帳戶被盜用會導致負面新聞報導、用戶數量下降，並對**品牌聲譽造成長期損害**。

防止帳號盜用攻擊

保護敏感資料

防止未經授權存取公司和客戶的機密資訊。

保護帳戶隱私

確保採取強有力的安全措施來保護客戶帳戶和個人資料。

維持業務連續性

最大限度減少因帳戶被盜用造成的干擾，以確保營運順利進行。

監控高階主管帳戶

監控關鍵高階主管和重要人士的帳戶，以降低貴公司最受矚目的威脅風險。

帳號盜用常見問題

● 帳戶盜用保護值得購買嗎？

是的，帳戶盜用防護至關重要，因為從歷史經驗來看，這是對企業危害最大的攻擊之一。一旦**完全控制了您的帳戶**，犯罪分子就可以散佈惡意軟體、實施網路釣魚攻擊、盜取資金，並利用公司帳戶造成長期損害。

● 帳戶盜用和身分盜竊有什麼不同？

身分盜竊是指惡意行為者冒充他人身分的一系列風險。帳戶盜用（ATO）是身分盜竊的特定類型，指**網路犯罪分子未經授權存取現有帳戶**。因此，雖然身分盜竊可能涉及建立全新的詐欺帳戶，但帳戶盜用則是利用現有帳戶進行攻擊。

● 啟用多因素身份驗證足以防止帳戶被盜用嗎？

多因素身份驗證 (MFA) 是加強帳戶安全性的有效方法，但不足以防止帳戶盜用 (ATO)。帳戶盜用可能由多種駭客技術造成，例如**會話劫持，這些技術可以繞過 MFA 安全措施**。例如，駭客可以控制您的 MFA 設備或攔截安全碼。為了防止帳戶盜用，最好將 MFA 與其他安全措施結合使用。

● 帳戶被盜用有哪些危險訊號？

帳戶資訊變更通常是犯罪分子試圖盜用帳戶的主要跡象。犯罪者通常會嘗試更改帳戶的主要郵箱、電話號碼、備用郵箱，以及從新的地點購物。

● 哪些行業最容易遭受帳戶盜用攻擊？

大多數行業都容易遭受帳戶盜用攻擊，但零售、遊戲、醫療保健以及金融和線上服務業的公司往往是最主要的攻擊目標。

● 如果我的組織帳戶在暗網上被發現，我該怎麼辦？

如果貴組織的帳戶出現在暗網上，請**重設洩漏的密碼並啟用強式驗證措施。您還應該調查憑證洩露的原因，並監控帳戶和網路中的可疑活動**。為防止未來再次發生類似事件，請強制執行嚴格的密碼策略，對員工進行網路釣魚威脅的培訓，並使用 Nordstellar 等威脅暴露管理平台進行監控。

會話劫持預防

識別被盜的活動會話 cookie
使受損會話無效
檢測受感染的設備

什麼是會話劫持？

會話劫持是一種網路攻擊，攻擊者可以利用它未經授權的方式存取使用者在網站或應用程式上的活動會話。會話劫持是如何運作的呢？它也稱為 Cookie 劫持，其原理是竊取活動會話 Cookie，這是網站保存在您裝置上的臨時檔案。這些 Cookie 包含您的身份驗證訊息，因此攻擊者無需重新輸入您的登入資訊或完成其他身份驗證步驟（例如雙重認證 (2FA)、多因素身份驗證 (MFA) 和密碼驗證），即可使用您的線上帳戶。

如何防止會話劫持

● 系統更新

保持系統和應用程式更新。**及時修補跨站腳本 (XSS) 和其他漏洞有助於保護會話 cookie**，即使 cookie 被盜也能防止會話劫持。

● 訓練

額外的安全措施和軟體修補程式無法解決的問題，可以透過教育來解決。**確保公司裡的每個人都能識別網路釣魚攻擊**，並了解各種社會工程技巧。

● 防火牆

防火牆通常是保護系統免受未經授權存取的第一道防線。請確保您的防火牆和防毒軟體**配置正確**，以確保它們能夠阻止惡意攻擊。

● 裝置綁定會話

將**會話限制在特定裝置、IP 位址或瀏覽器指紋範圍內**。這樣可以大幅增加攻擊者重複使用竊取的 Cookie 的難度。或者，如果使用者從新裝置登錄，則通知使用者。

● 安全連線

始終**使用 HTTPS 加密使用者與系統之間交換的資料**。此外，盡可能避免在沒有 VPN 的情況下使用公共 Wi-Fi。不安全的網路通常是網路犯罪分子的目標。

● NordStellar

在威脅暴露管理方面，像NordStellar這樣的平台可以為您完成大部分工作。**透過監控深網和暗網，它可以偵測受惡意軟體感染的裝置、識別被盜的cookie並使受損會話失效**。

會話劫持防護機制運作

全天候監控暗網
掃描深網和暗網，尋找與組織員工和客戶相關的被盜會話 cookie。

使被竊的會話 cookie 失效
撤銷被入侵的會話，並防止攻擊者劫持這些會話。

通知有關被盜 Cookie 的信息
當平台偵測到被盜的會話 cookie 時，您將收到警報，包括來源、裝置和其他被盜資訊。

會話劫持如何防護

防止未經授權存取敏感數據

會話劫持防護透過**偵測和失效被盜的會話 cookie**來確保公司帳戶的安全。

保護您的公司免受網路詐欺

此解決方案可防止攻擊者**使用竊取的會話 cookie** 進行帳戶欺詐，例如未經授權的交易和身分冒用。

保障您的企業資源安全無虞

它確保**未經授權**的各方無法存取公司資源，包括基於雲端的應用程式和內部網路。

會話劫持常見問題

● 會話劫持是如何運作的？

會話劫持始於會話 ID 盜竊，即**竊取使用者的活動會話 cookie**。常見方法包括嗅探未加密流量、跨站腳本攻擊 (XSS) 或惡意軟體。
然後，攻擊者利用竊取的會話 ID 來偽造使用者身分。換句話說，攻擊者欺騙系統，使其誤以為自己是合法使用者。
一旦入侵成功，他們就可以利用這種存取權繼續會話而無需重新輸入密碼。他們可以存取敏感資訊、執行未經授權的操作或提升權限。

● 會話劫持有多危險？

會話劫持非常危險，因為**攻擊者可以完全控制使用者的帳戶**。利用被盜用的帳戶，他們可以竊取受害者的身份信息，訪問並洩露公司內部數據，甚至授權交易。對於任何企業而言，財務和聲譽損失都將十分巨大，而且很可能導致監管罰款

● 如何偵測會話劫持？

偵測會話劫持通常歸結為尋找警告訊號，例如異常的帳戶活動、突然登出以及來自未知裝置的同時登入警報。
NordStellar 可以透過監控會話完整性、提醒使用者註意可疑活動以及使受損會話失效來幫助緩解這些威脅。

● 如何選擇最佳的會話劫持防護方案？

要選擇最佳的會話劫持預防方案，請尋找信譽良好的品牌，該品牌應**提供強大的加密、會話監控和一定程度的自動化功能**。

● 最常見的會話劫持技術有哪些？

會話劫持技術有多種類型。最常見的有會話固定、會話側劫持、跨站腳本攻擊和惡意軟體攻擊。

會話鎖定是指誘騙使用者使用駭客已知的會話 ID，而會話劫持則需要透過未加密的網路竊取會話 ID。
駭客通常也會使用惡意軟體來捕獲儲存在受感染裝置上的會話 cookie，或向網站注入惡意腳本。

● 如果您收到會話劫持通知，該怎麼辦？

如果您收到會話劫持通知，請立即登出您的帳戶。此外，請**務必更改密碼、啟用多因素身份驗證 (MFA) 並聯絡您公司的網路安全團隊**。

外部漏洞掃描

- 縮小企業的攻擊面
- 漏洞一旦發現就立即修補
- 加強安全防範

什麼是外部漏洞掃描？

外部漏洞掃描是一種幫助偵測網路中面向網路部分的漏洞的過程。它就像一個互聯網連接設備的搜尋引擎，從公開來源（例如服務橫幅、連接埠和自由廣播的網路流量）收集資料。該掃描器有助於發現所有面向外部資產中的各種漏洞、缺少的安全性修補程式和過時的軟體。

NordStellar 從攻擊者的角度執行外部掃描，試圖在無法存取網路的情況下尋找網路漏洞。

漏洞掃描運作

1

發現資產

我們的漏洞掃描器將利用 **DNS 枚舉、CRT.sh 抓取和其他自動化流程**，繪製貴公司的攻擊面圖，並識別與您的網域關聯的資產。

2

掃描連接埠

我們會**檢查與您的網域相關的所有資產是否存在開放連接埠**—這些連接埠通常會隱藏安全漏洞。如果掃描發現開放端口，也會檢查哪些服務正在使用該端口。

3

識別漏洞

下一步是檢查漏洞。我們的平台**利用 Shodan 龐大的漏洞資料庫和豐富的 CVE 數據**，尋找與開放連接埠相關的任何漏洞。

4

風險優先排序

一旦發現漏洞，我們的平台將**使用 CVSS v3、CVSS v2 和 EPSS 評分系統**來評估每個安全弱點的嚴重性和影響。

5

呈現結果

最後，NordStellar 提供**詳細的漏洞掃描結果**。為了盡可能提高結果的針對性，該平台會根據風險等級提供優先排序的威脅清單。您也可以根據自身需求自訂警報。

外部漏洞掃描偵測到那些問題?

開放埠

發現開放連接埠並**保護透過這些連接埠**運行的服務免受暴露。

過時的軟體

了解您的軟體哪些部分**未能更新並修復已知漏洞**。

配置錯誤

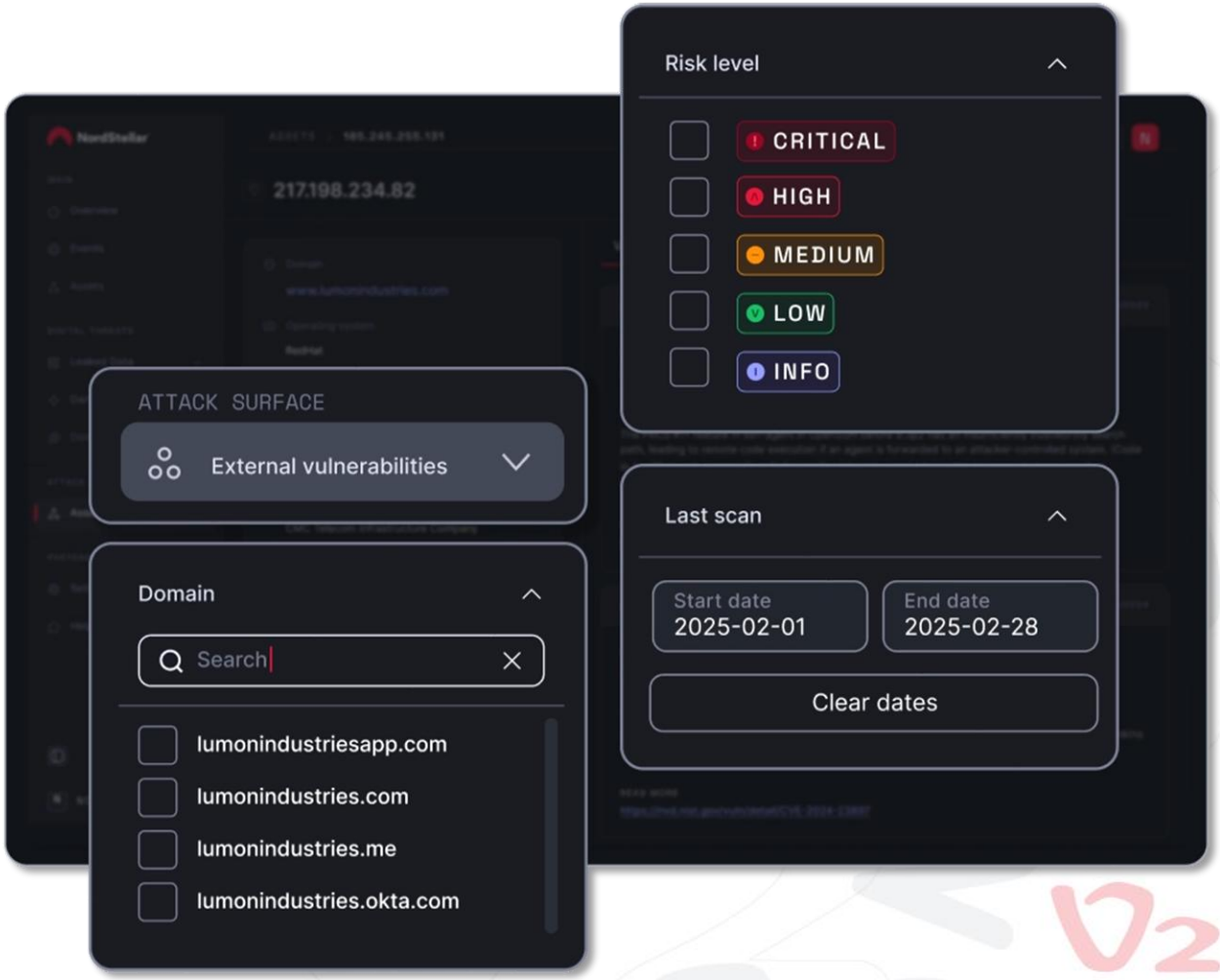
識別並處理身份驗證問題、過於寬鬆的防火牆以及**設定不當**的安全參數。

未受保護的 API

找出有缺陷的API，並保護那些駭客**無需身份驗證**即可從網路存取的API。

如何使用NordStellar掃描漏洞?

您只需向我們的漏洞掃描器**提供貴公司的網域名稱即可**。掃描器隨後將自動啟動資產發現功能，尋找所有相關的子網域和 IP 位址。攻擊面映射完成後，**掃描器將定期分析您的基礎設施，並在發現任何漏洞時發出警報**。 NordStellar 可讓您按漏洞類型和風險等級自訂安全警報，或選擇您希望接收通知的特定情況。



外部漏洞掃描優勢

● 主動安全監控

領先一步，防範下一次網路攻擊 - 使用 NordStellar 的漏洞掃描器，**準確清點您暴露在網路上的資產**。它能幫助您在安全漏洞的早期階段就發現它們，並揭露隱藏在影子基礎設施中的資產。從而為您爭取更多時間來應對不斷增長的風險，並減輕潛在的損失。

● 可自訂通知

立即取得已**發現漏洞或受影響服務的通知並採取行動**。您可以根據漏洞類型和嚴重程度自訂安全警報，並選擇在特定安全事件發生時接收通知。透過電子郵件、平台內通知或其他安全工具接收安全警報。

● 有效發現漏洞

NordStellar 的外部威脅掃描器涵蓋多種漏洞，包括**開放連接埠、正在運作的服務和技術以及配置錯誤的防火牆**。掃描結果還會提供有關已發現漏洞的詳細信息，包括漏洞描述、CVE ID、CVSS 評分、風險等級、受影響的服務以及建議的修復措施。

● 更高的合規標準

遵守各項行業法規需要定期進行漏洞評估，NordStellar 可以幫助您實現這一目標。讓您的公司達到**更高的合規標準—透過定期提交外部漏洞報告**，展現您抵禦網路威脅的能力。

外部漏洞掃描常見問題

● 為什麼外部漏洞掃描很重要？

外部漏洞掃描器能夠識別系統和網路中面向互聯網部分的漏洞。這使得企業能夠在**安全風險的早期階段發現並修復漏洞**，防止網路犯罪分子利用這些漏洞。

● 什麼是漏洞優先排序？

漏洞優先排序是指根據**漏洞的嚴重程度、潛在影響和被利用的可能性對其進行排名**。優先排序有助於企業在為時過晚之前發現並解決最緊迫的漏洞。

● 應該多久執行一次外部漏洞掃描？

漏洞掃描頻率越高越好。但是，您至少應該每季對外部資產進行一次安全風險掃描。這有助於控制企業的攻擊面，並讓您主動維護公司安全。

使用 NordStellar，您可以**安排漏洞掃描以固定時間間隔（例如每天或每週）自動運行，也可以根據需要手動啟動掃描**。

● 執行漏洞掃描後，下一步該怎麼做？

一旦發現現有或新增漏洞，應立即指派**相關安全團隊透過套用安全性修補程式、更新或配置來修復安全風險**。然而，您可能無法立即修復系統中的所有故障。在這種情況下，應實施適當的緩解策略，以降低漏洞暴露風險並減少遭受攻擊的可能性。

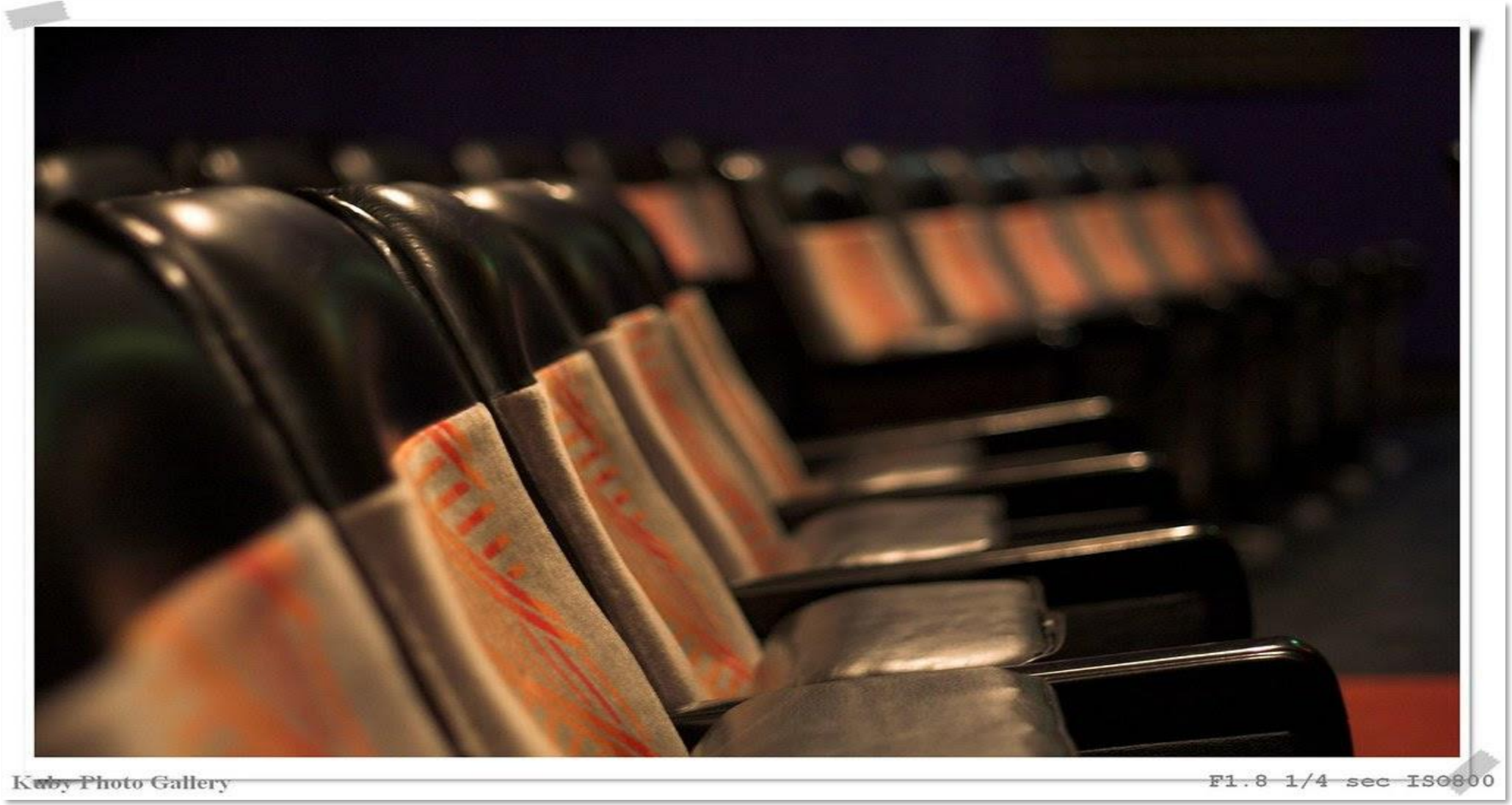
● 掃描外部漏洞能否幫助實現合規性？

外部漏洞掃描可以幫助您**滿足法規和標準中關於定期安全檢查的要求，並及時提示您解決系統缺陷**。

● 內部漏洞掃描和外部漏洞掃描有什麼不同？

外部漏洞掃描會檢查企業面向網際網路的資源，例如網站和伺服器。它有助於偵測攻擊者通常針對企業網路外部發動的攻擊漏洞。而內部漏洞掃描則著重於企業內部網路的薄弱環節，包括員工可以存取的系統、設備和應用程式。

演示



使用NordStellar 偵測並預防暗網威脅

- **NordStellar是什麼？**

NordStellar是一個以企業為導向的威脅暴露管理平台。它可以幫助您更快地偵測出受損的客戶和員工數據，做好應對網路攻擊的準備，並避免網路威脅。

- **我該如何開始使用NordStellar？**

只需與我們的團隊預約演示，即可了解 NordStellar 如何滿足您的業務需求。

- **NordStellar是否支援任何整合？**

是的，NordStellar 的 API 可以與各種 SIEM 和 SOAR 平台進行廣泛的集成，例如 Splunk、QRadar、Datadog、Fortinet、Sentinel、Elastic 或 Cortex。


Q&A

相關連結

- NordStellar https://nordstellar.com/
- 公開資訊觀測站 https://mopsov.twse.com.tw/mops/web/t05sr01_1