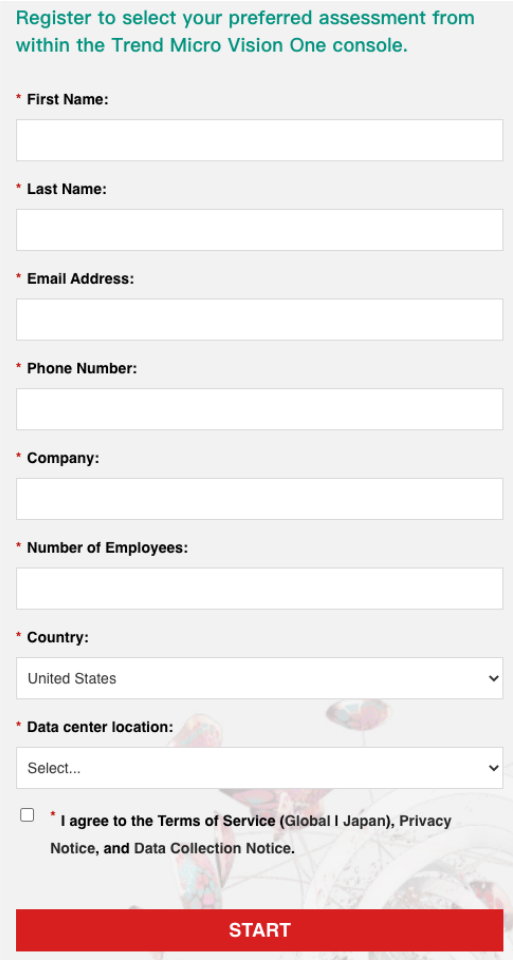
Trend Micro Security Assessment Service 試用申請

申請 URL

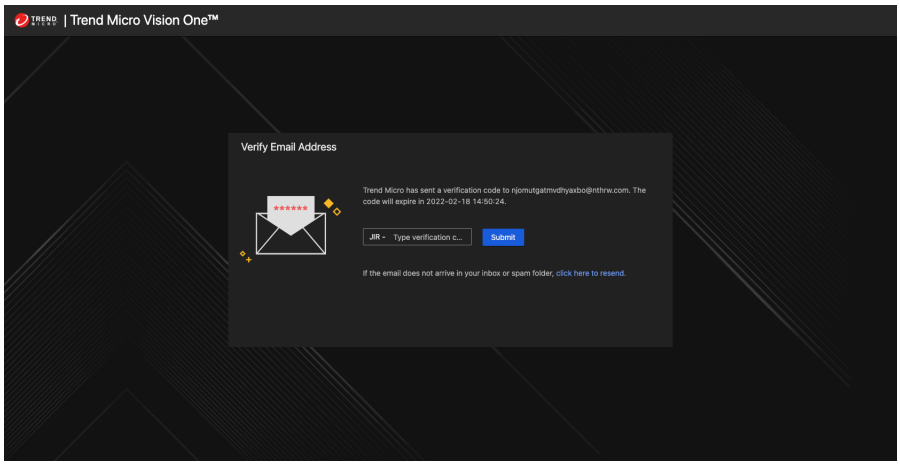
https://resources.trendmicro.com/security-assessment-service-us.html

填入相關申請資訊

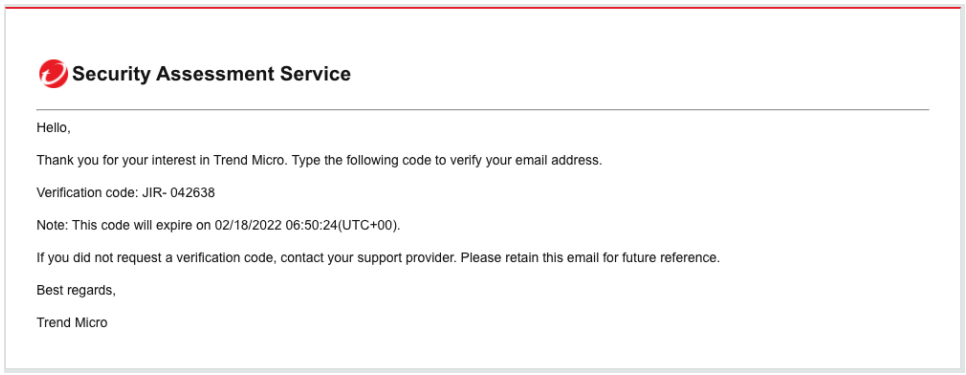


Data Center Location 台灣客戶建議使用 Singapore

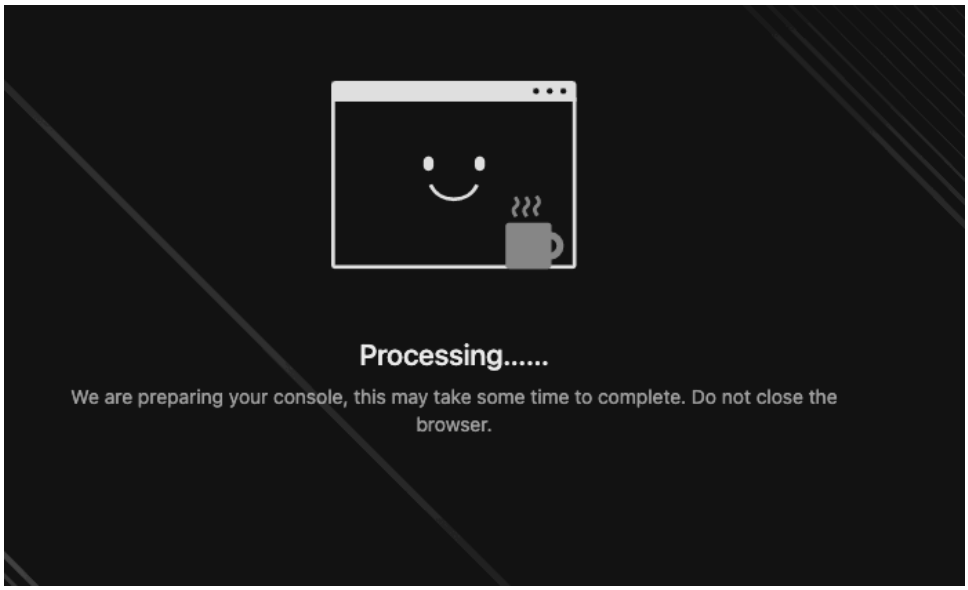
完成資料填入後點擊”Start”，系統會出現要求輸入驗證碼



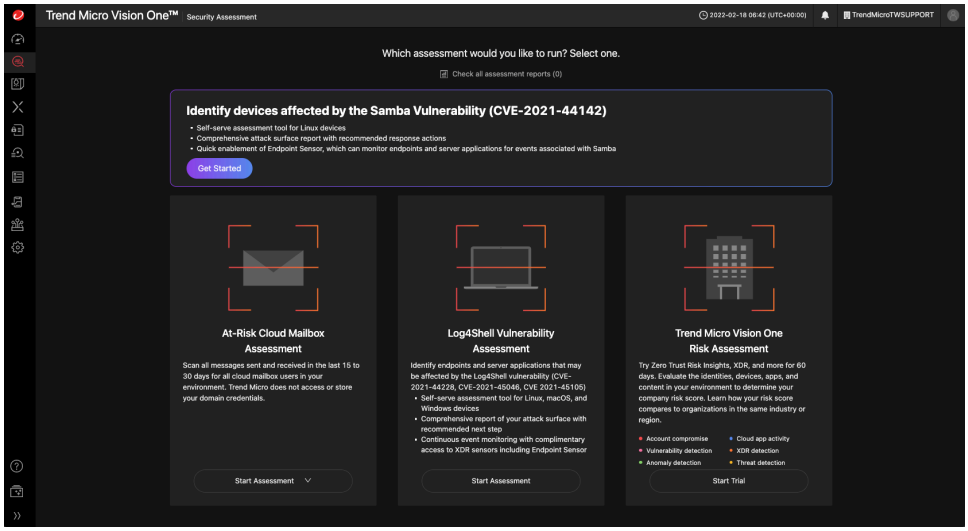
請確認您的信箱有收到來自趨勢科技發出的驗證碼信件，並且輸入信件中提供的驗證碼. 請注意，驗證碼有時效性，若超過時效，請點擊上述步驟畫面中”Click to resend”重新寄送驗證碼・



驗證碼輸入完畢且正確，系統將會開始建立全新趨勢科技 VisionOne 平台.



等待建立完成後，您將會自動登入到 VisionOne 平台



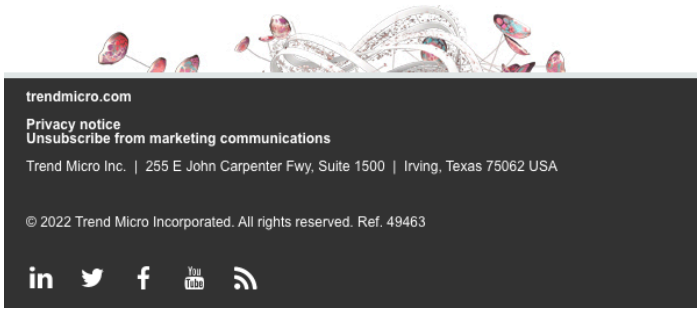
同時，您也會收到一封註冊成功的信件

Thank you for registering for the Trend Micro Security Assessment Service. Using the Tren d Micro Vision One™ platform, this complimentary service offers insight into your attack su rface, identifies potential threats in your environment and provides a detailed, downloadabl e report with recommended response actions.

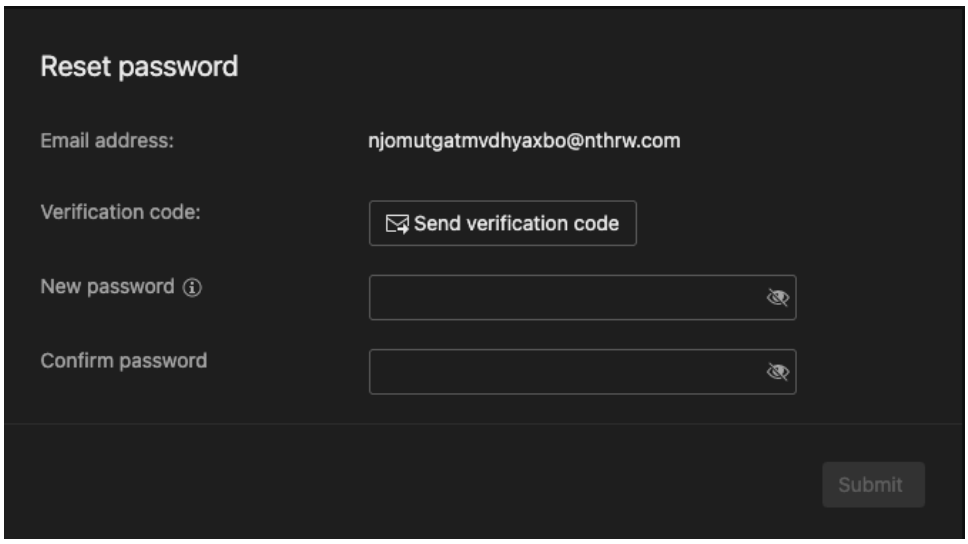
Start assessment

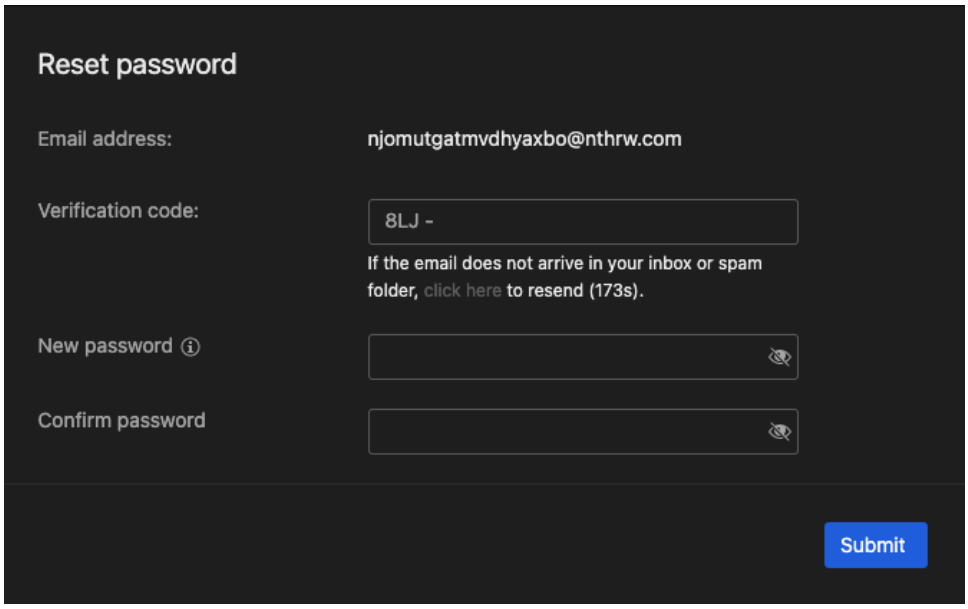
You have the option to extend your assessment to trial XDR sensors for endpoint, server, email, and network to continuously monitor, detect and respond to attacks for free for 60-d ays after sign-up.

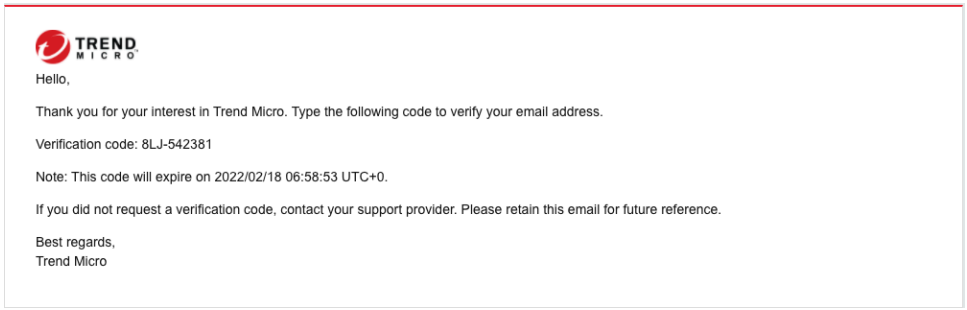
Thank you,
The Trend Micro Team

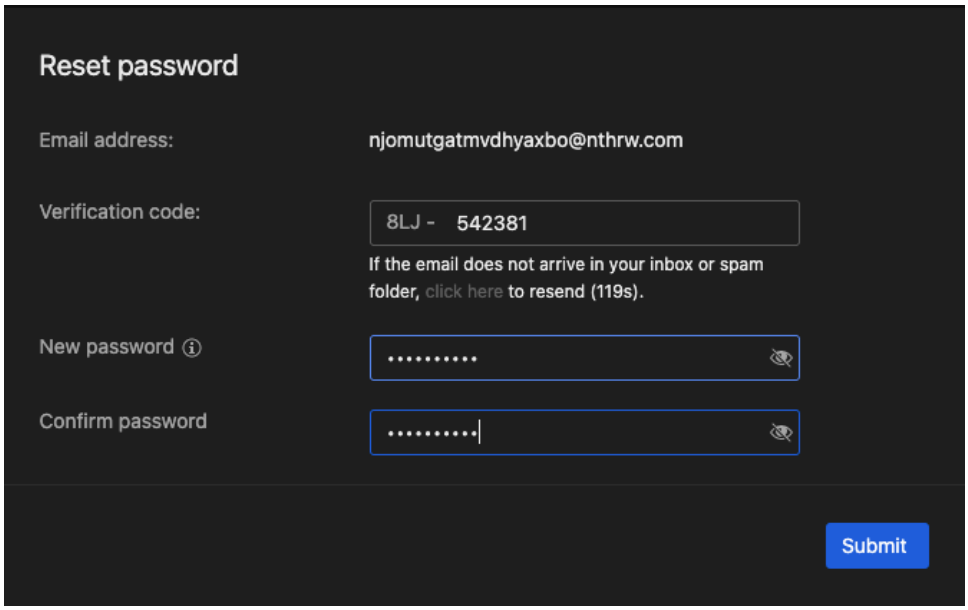


請點擊信件中”Start assessment”的按鈕進行密碼重新設定步驟
點擊後會出現 Reset password 的畫面，請點擊”Send verification code”

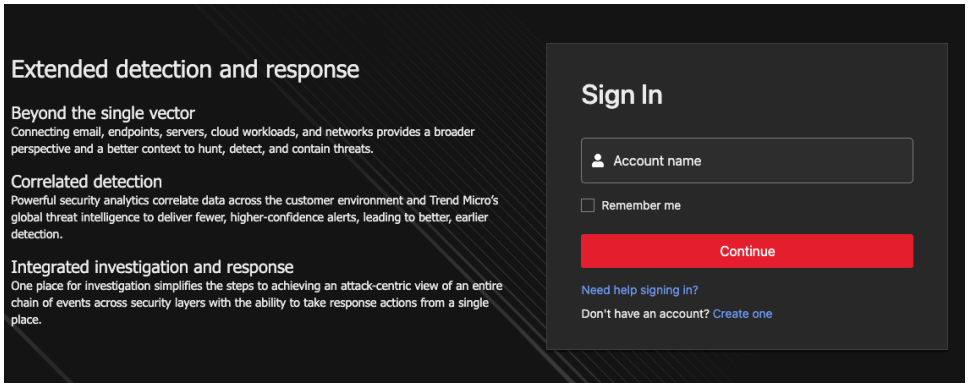

Reset password
Email address:
njomutgatmvdhyaxbo@nthrw.com
Verification code:
Send verification code
New password
Confirm password
Submit


Reset password
Email address:
njomutgatmvdhyaxbo@nthrw.com
Verification code:
8LJ -
If the email does not arrive in your inbox or spam folder, click here to resend (173s).
New password
Confirm password
Submit

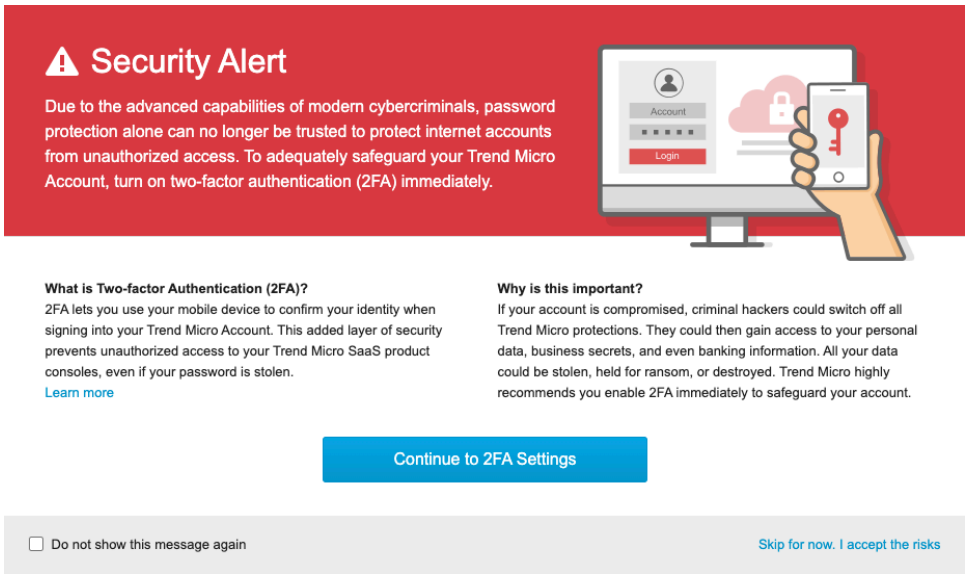

TREND MICRO
Hello,
Thank you for your interest in Trend Micro. Type the following code to verify your email address.
Verification code: 8LJ-542381
Note: This code will expire on 2022/02/18 06:58:53 UTC+0.
If you did not request a verification code, contact your support provider. Please retain this email for future reference.
Best regards,
Trend Micro



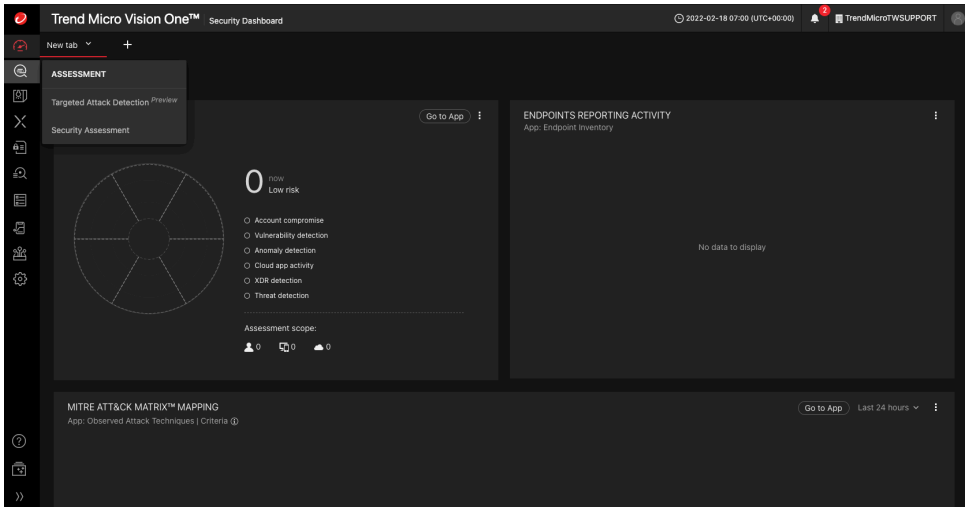
Submit 後返回登入頁面，登入帳號請填入申請的 Email Address



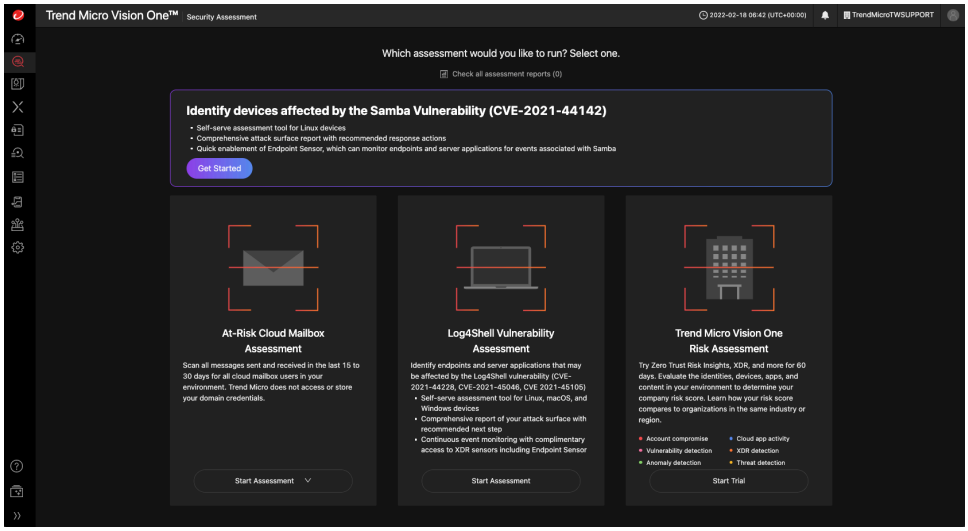
輸入 Reset 後的密碼登入，登入後系統會提醒是否啟用兩階段驗證功能，若不需要，可以點擊畫面中右下角”Skip for now, I accept the risks”



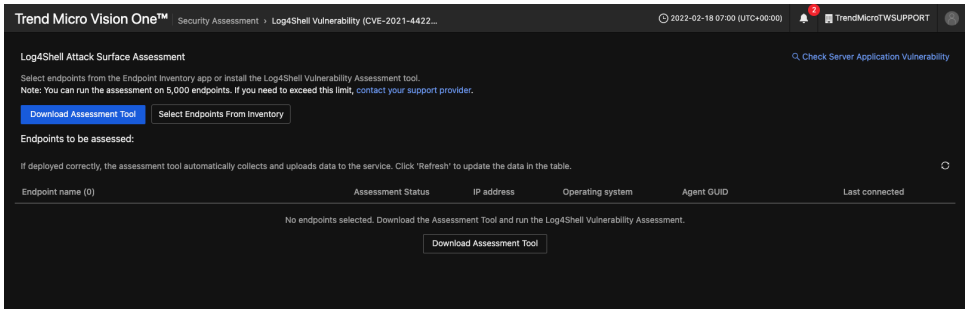
點擊左側功能 APP 此圖示  選擇”Security Accessment”開始進行檢測



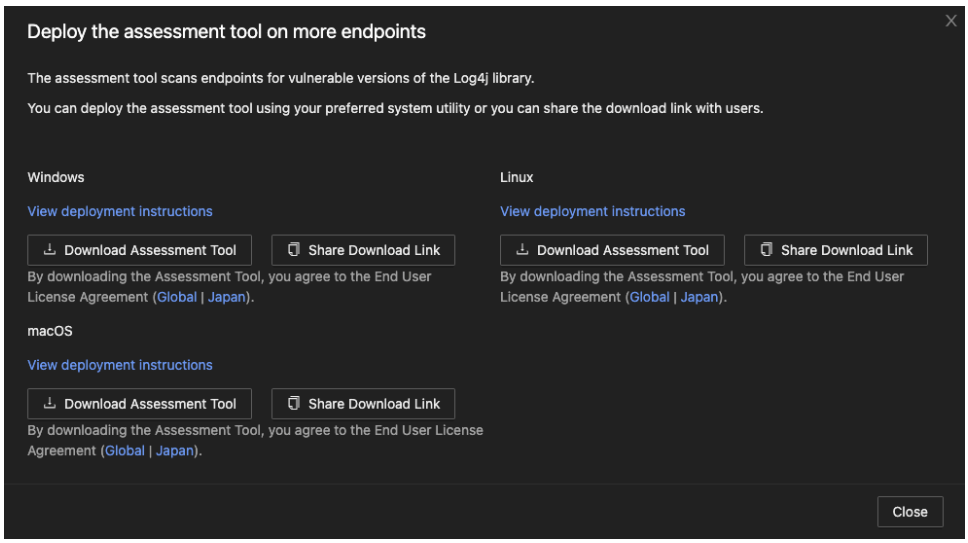
您可以依據您目前的需求進行檢測，以畫面中我們選擇”Log4Shell”弱點來進行檢測



選擇”Download Assessment Tool”



選擇需要檢測的作業系統平台來進行檢測

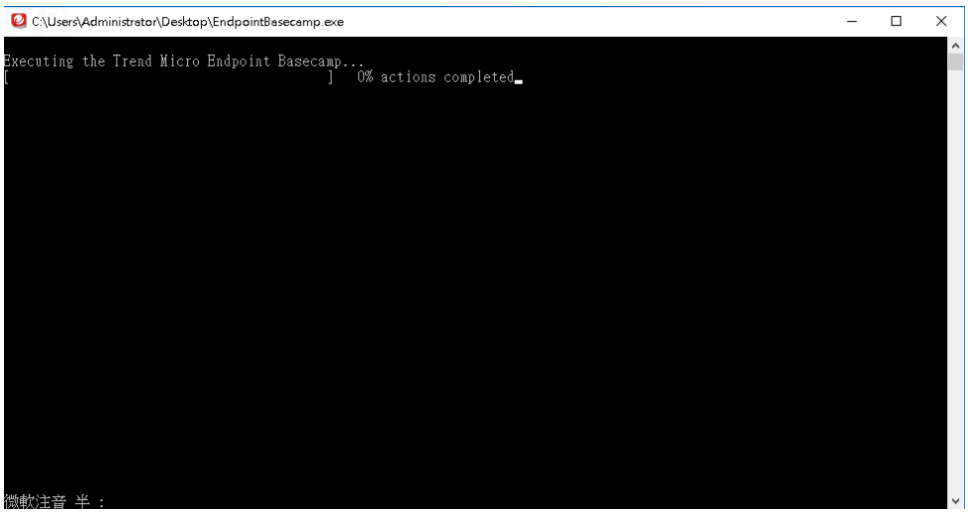


我們以 Windows 平台來舉例，您可以選擇下載 Assessment Tool 後分享安裝，或是分享下載連結給其他使用者下載安裝。

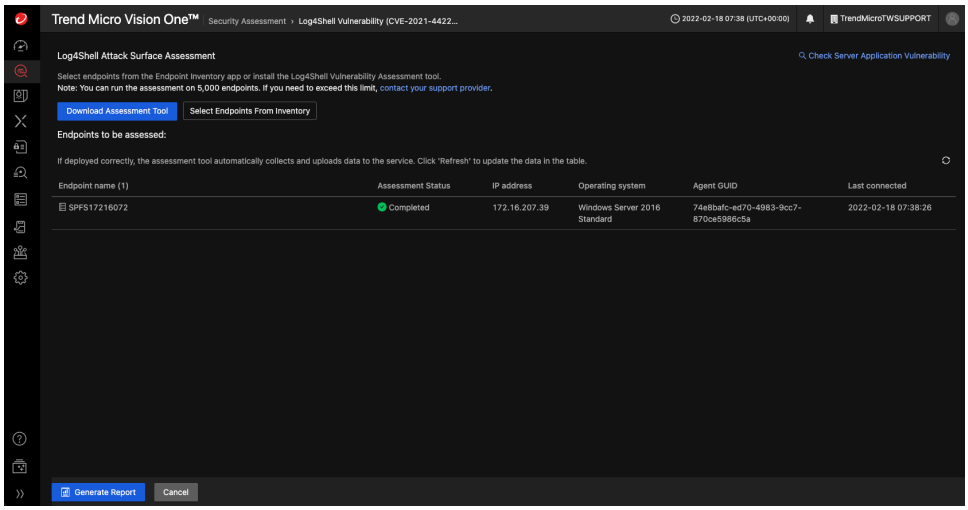
NOTE:請注意此工具僅能在貴公司環境中使用，若其他非貴公司環境中使用相同的檢測工具，會造成資料不正確的情況。

工具下載後，建議請使用系統管理者權限執行”EndpointBasecamp.exe”

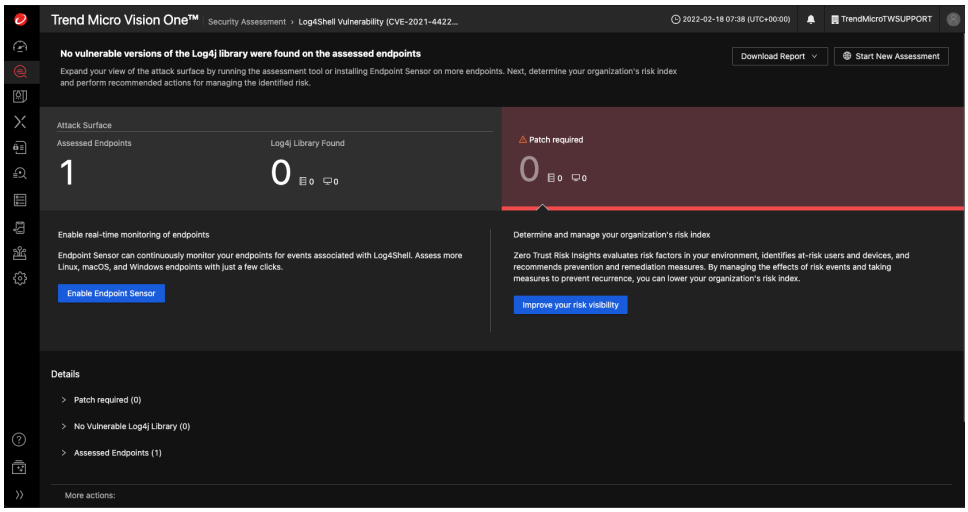
執行後會出現檢測視窗，請勿關閉該視窗，執行完畢後該視窗會自行關閉。



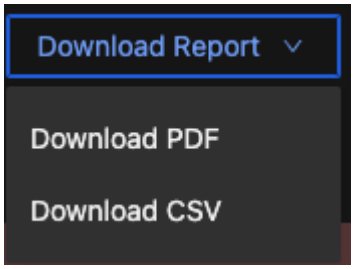
檢測完畢後將會出現在列表中，等待全數執行的主機都完成檢測



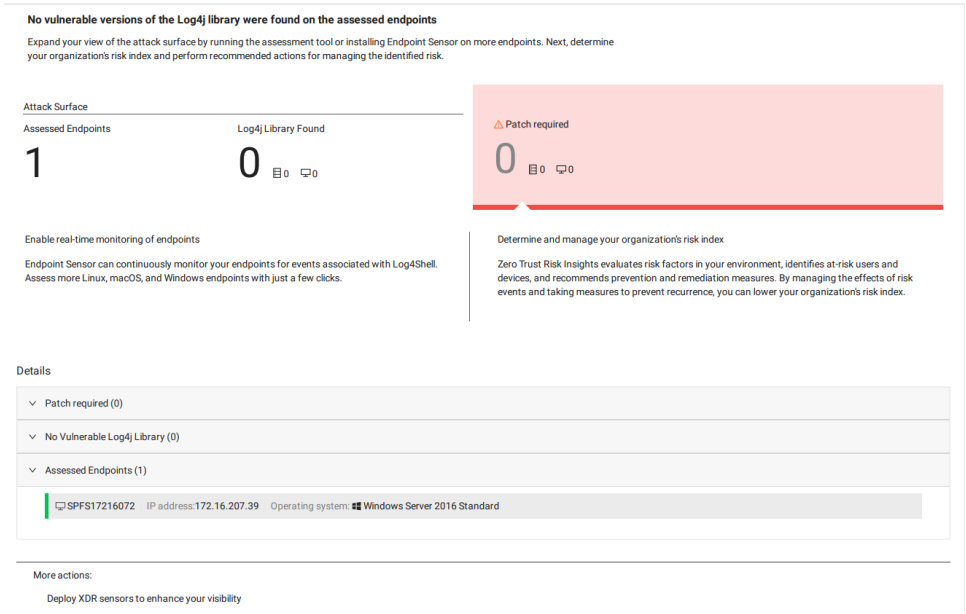
檢測完畢後，點擊下方”Generate Report”按鈕來產生報表，報表中可以清楚告知有哪些主機是需要進行安裝安全性修補程式。



您也可以點擊”Download Report”選擇您所需要的報表格式



PDF Report 樣式

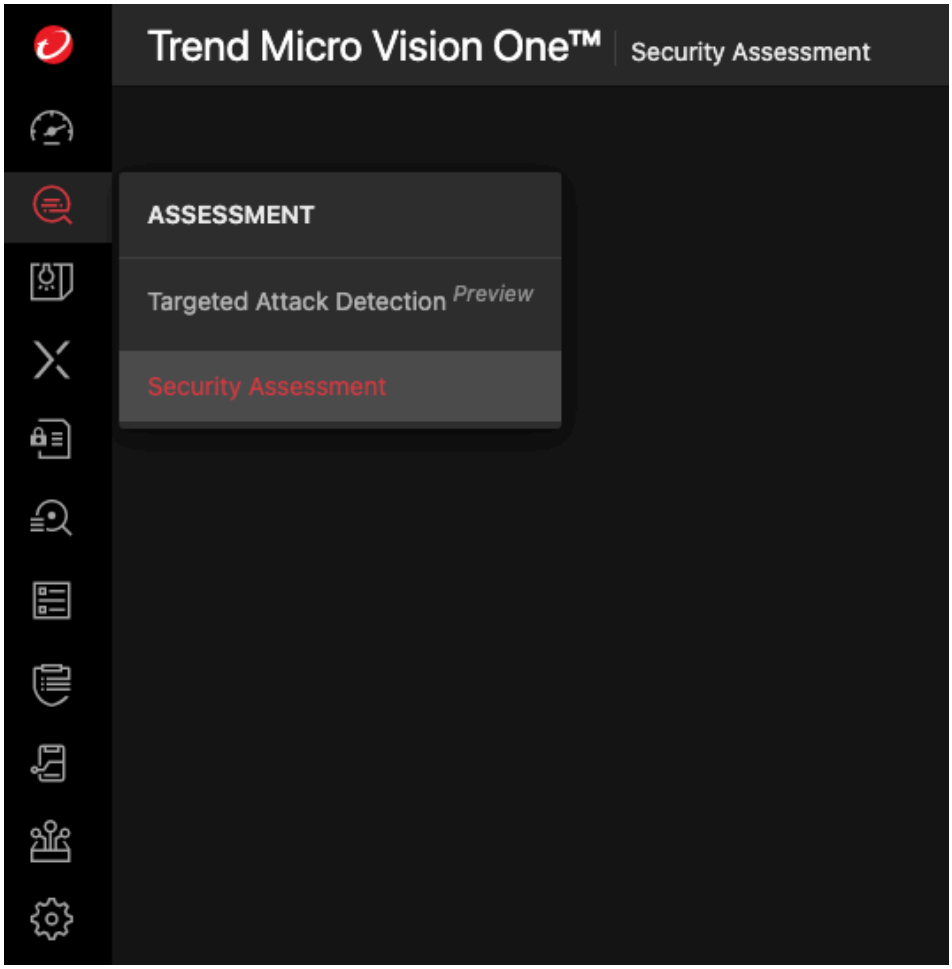


CSV Report 樣式

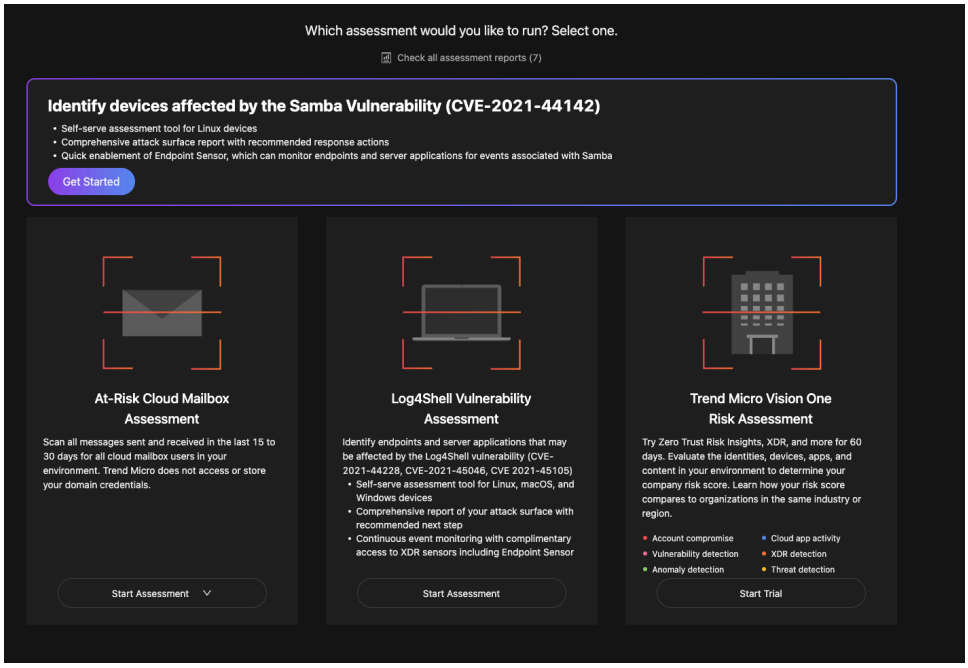
	A	B	C	D	E	F
1	hostname	ip address	file path	OS version	Last scan time	Status
2	SPFS17216072	172.16.207.39		Windows Server 2016 Sta	2022-02-18T07:38:12.000Z	Not Found
3						

正式客戶使用說明

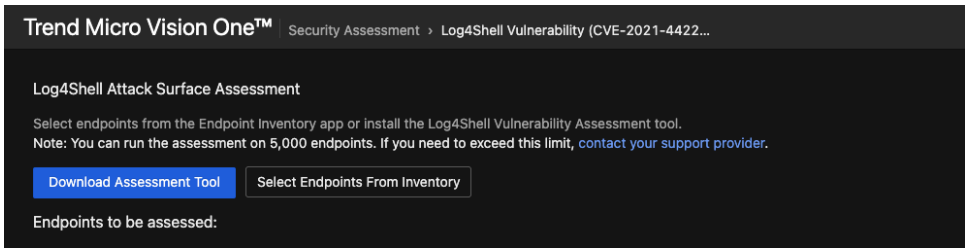
點擊左方 App 工作列，選擇到”Assessment | Security Assessment”



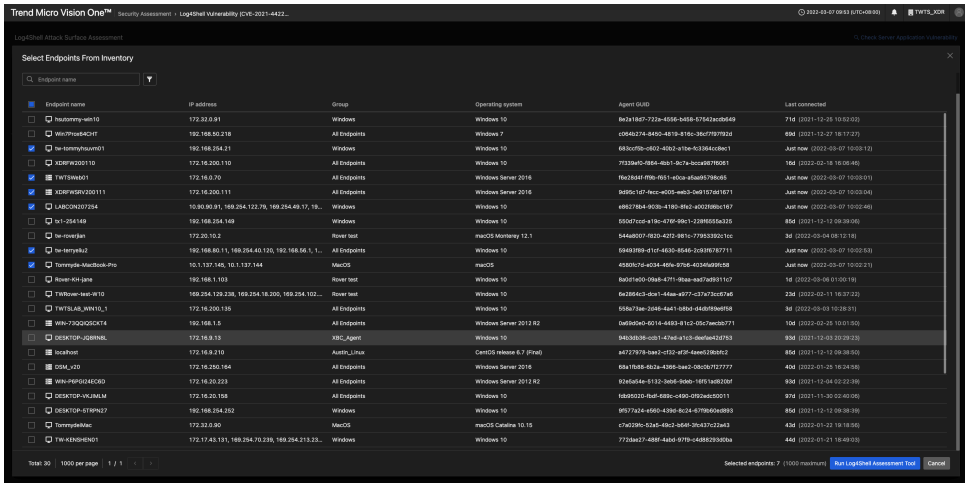
依照你的需求選擇檢測項目



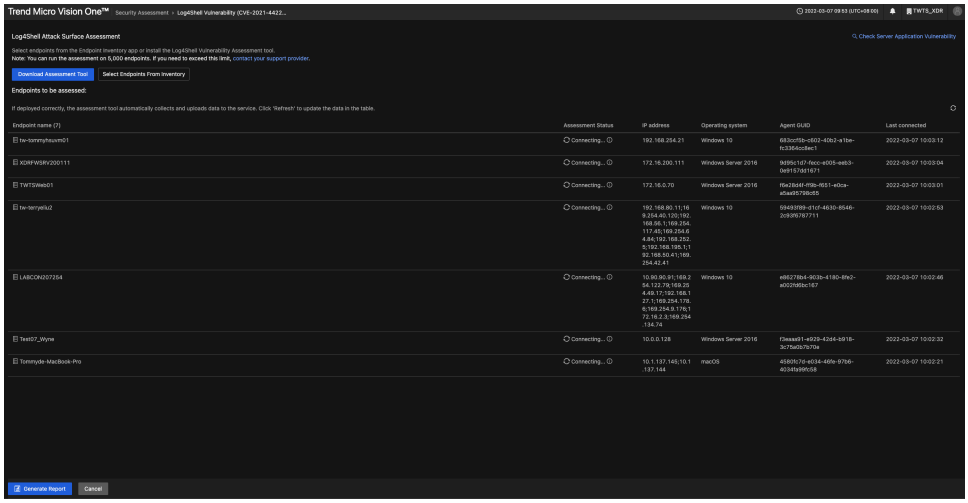
範例為使用 Log4shell 的檢測，點擊”Start Assessment”後，可選擇已經連線上 Vision One 平台中的 Endpoint Inventory 中的主機進行檢測，



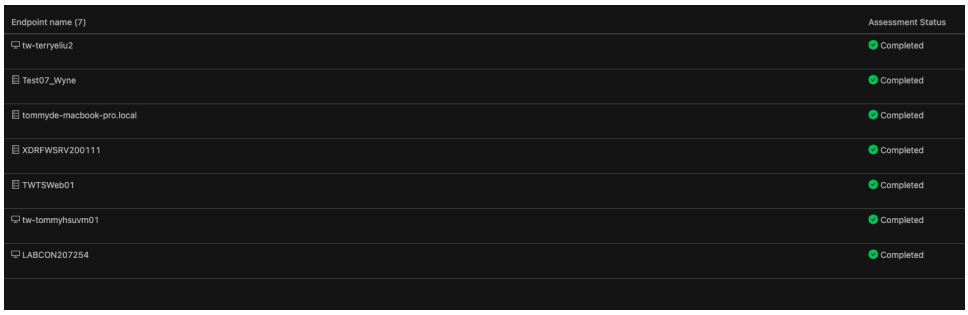
選擇完畢後點擊”Run Log4J assessment Tool”



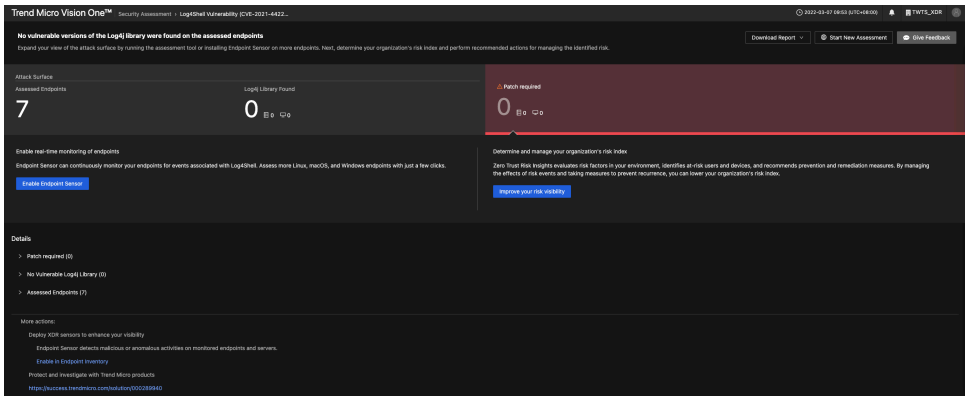
Vision One 平台即可開始進行相關檢測



完成檢測後，可以點擊”Generate Report”產出報表


Endpoint name (7)
Assessment Status
tw-terryeliu2
Completed
Test07_Wyne
Completed
tommyde-macbook-pro.local
Completed
XDRFWSRV200111
Completed
TWTSWeb01
Completed
tw-tommyhsuvm01
Completed
LABCON207254
Completed

報表即可呈現檢測結果


Trend Micro Vision One™
Security Assessment
Log4Shell Vulnerability (CVE-2021-4422...
TWTS_XDR
No vulnerable versions of the Log4j library were found on the assessed endpoints
Expand your view of the attack surface by running the assessment tool or installing Endpoint Sensor on more endpoints. Next, determine your organization's risk index and perform recommended actions for managing the identified risk.
Download Report
Start New Assessment
Give Feedback
Attack Surface
Assessed Endpoints
7
Log4j Library Found
0
Patch required
0
Enable real-time monitoring of endpoints
Endpoint Sensor can continuously monitor your endpoints for events associated with Log4Shell. Assess more Linux, macOS, and Windows endpoints with just a few clicks.
Enable Endpoint Sensor
Determine and manage your organization's risk index
Zero Trust Risk Insights evaluates risk factors in your environment, identifies at-risk users and devices, and recommends prevention and remediation measures. By managing the effects of risk events and taking measures to prevent recurrence, you can lower your organization's risk index.
Improve your risk visibility
Details
Patch required (0)
No Vulnerable Log4j Library (0)
Assessed Endpoints (7)
More actions:
Deploy XDR sensors to enhance your visibility
Endpoint Sensor detects malicious or anomalous activities on monitored endpoints and servers.
Enable in Endpoint Inventory
Protect and investigate with Trend Micro products
https://success.trendmicro.com/solution/000289940