DARKTRACE

FAQ:

Darktrace PREVENT

2023

https://darktrace.com

DARKTRACE

目錄


DARKTRACE
004.738.5
Günter Born
INTERNET
Łatwy start dla seniorów
Günter Born
INTERNET
Łatwy start dla seniorów
100 sposobów na GOOGLE

PREVENT 產品系列

Q1. 什麼是Darktrace PREVENT?

Darktrace PREVENT是在最需要的地方加強安全防禦。當資安團隊面臨時間和預算限制時，Darktrace PREVENT旨在幫助他們回答的問題是「如果我有1美元的資安預算，或者資安團隊只有1小時的時間，如何最有效的利用資源？」

每個組織的風險狀態是獨特的，尤其擁有的資產、資安策略和部署的技術等因素決定。PREVENT不會只是呈現一個適用於該組織的已知漏洞清單。它會察覺可進入組織的每個潛在入口（ASM），並測試（例如嘗試闖進入）這些入口，以找出哪些入口對這個特定組織（E2E）具有最高的潛在影響力。

其結果是按潛在影響力優先排序風險的清單。簡言之，PREVENT告訴CISO和IT團隊在哪裡投資時間、精力和預算去填補漏洞或解決弱點。

Darktrace PREVENT是一個產品系列，由2個產品組成：

1. PREVENT / **Attack Surface Management**
   或
   PREVENT / **ASM**
2. PREVENT / **End-to-End**
   或
   PREVENT / **E2E**

作爲Cyber AI Loop的一部分，Darktrace PREVENT將其發現的資訊傳遞給Darktrace DETECT和Darktrace RESPOND（更多訊息請參見下文）。

Q2. PREVENT的每個產品的功能是什麼？

Darktrace PREVENT / ASM檢視一個組織外部/對接網路的一面，持續監控當前和新興的風險，包括影子IT、供應鏈風險、配置錯誤和已知漏洞。

Darktrace PREVENT / E2E集成了多個最佳防禦能力，包括攻擊路徑建模、滲透測試增強、入侵和攻擊仿真、安全意識測試和漏洞優先級別。

Q3. PREVENT如何與Darktrace其他產品配合使用？

PREVENT提供資訊給Darktrace DETECT和RESPOND，以加強和增強這些產品的防禦能力。

例如：

- PREVENT可以預先警告Darktrace/ Email有關冒充組織的惡意網域。
- Cyber AI Analyst可以使用從PREVENT / ASM獲取的外部數據來增強其調查功能。反之，Darktrace DETECT和RESPOND產生的輸出會反饋到PREVENT中。這些產品形成一個反饋「循環」，不斷增強組織的整體安全韌性，並隨時間持續學習。

Q4. PREVENT會讓DETECT和RESPOND過時嗎？

不會，PREVENT是一個完全不同的功能。相反地，它可以通過提高這些產品系列的準確性和精度，將DETECT和RESPOND的使用效率最佳化，並告知CISO和IT團隊在哪些方面需花費時間、精力和預算以彌補缺口或漏洞。

Q5. PREVENT是否取代了漏洞管理工具、滲透測試或紅隊攻擊演練？

Darktrace PREVENT擷取了這些工具的優點，融合了AI技術，結合成一個全面的點到點解決方案。相較於人力驅動的方法，PREVENT的涵蓋全面的範圍，並且持續進行調適，隨著組織的變化而改變，而不僅是提供單一的時間點分析。一些組織可能希望與Darktrace PREVENT同時併用其他資安措施。它不會取代人力驅動的測試，例如滲透測試和紅隊攻擊演練，但測試者或紅隊應用PREVENT可以增強他們的操作。

Q6. SIEM是否能夠接收PREVENT的數據？

可以。

PREVENT/ASM
產品價值與功能

Q7.當部署更動時，尤其是在雲端上，PREVENT是否能夠識別軟體漏洞？

PREVENT/ASM會持續監控整個攻擊面，包括軟體漏洞等風險。即便是在雲端的資產，也會識別並進行修復。

PREVENT/E2E也會考慮雲端和SaaS數據，提供相關攻擊路徑的資訊。

Q8. PREVENT部署有哪些要求呢？

ASM沒有任何要求。
我們只需要一個品牌名稱就可以了。
E2E有一些要求，
因爲它依賴於來自客戶部署的數據：

必須擁有（需滿足部署E2E的必要條件）

- 客戶使用M365（曾經的O365）作爲電子郵件供應商
- 客戶使用DETECT/Network

（僅限使用電子郵件客戶不符合資格）

可以擁有

（請提供相關內容，以便我們利用數據）

- 客戶使用Darktrace/Email
- 客戶使用Microsoft Defender、Crowdstrike、Sentinel One或Darktrace/Endpoint。

Q9. PREVENT/攻擊面管理 (ASM)是什麼？它如何幫助保護我的組織？

攻擊面是企業中所暴露於外的部分（即所有面向網路的資產）。

通過了解攻擊面的能見度，您可以從攻擊者的角度了解每個資產如何被利用爲進入您的組織的入口。

您可以通過持續監控攻擊面上的風險，優先處理高風險漏洞並採取行動來加強它們，從而在這些威脅前保持一步之遙，大幅降低您的網路風險。

Q10. ASM最常見的使用案例爲何？

請參閱使用案例文件以詳細瞭解以下每一個項目。以下內容由客戶的角度撰寫。

- **雲端和影子IT**：我是否能看到已經被創建或啟動的所有內容？
- **數據洩露和配置錯誤**：是否有不該存取的數據被存取？

- **供應鏈風險**：有哪些關於我供應鏈的資訊在網路上？我們留下了哪些供應商足跡？（換言之，攻擊者可以從可用資訊中推斷出什麼關於我方的技術（不僅是資安相關）？）是否有與我方品牌相關聯第三方網域存在風險（例如：Salesforce.Darktrace.com，Salesforce的Darktrace案例，該案例應該是由Salesforce保護的）？
- **品牌僞冒和釣魚**：尋找假冒我方的網站。
- **新漏洞**：例如Log4J。通過Darktrace，我們可以在幾秒鐘內知道我們的攻擊面是否受到這種漏洞的影響（而不是慌亂搜尋時常不完整的資訊）。
- **合規性**：我們可以自信地提供正在追蹤和完整攻擊面的報告。
- M&A：我們可以輕鬆地辨別與另一個IT基礎架構合併所帶來的新問題或風險。

Q11. 客戶通常從哪些使用案例開始？

PREVENT/ASM客戶通常從以下使用案例開始：

- **高風險問題**：解決問題並接收新的高風險問題警告。
- **影子IT**：找到高風險的陰影IT，並確保沒有新的影子IT被創建。
- **資產管理**：確保每個重要資產都有管理者，可以透過與CMDB系統整合或在PREVENT/ASM平台內實現。

Q12. PREVENT/ASM多久會「跑」一次？

PREVENT/ASM持續運作，但部分或底層資訊來源的更新可能有所不同。最後更新日期會顯示在UI。

Q13. PREVENT/ASM是否會有誤報？

不會。每個報告都有其原因，並且會提供技術證據解釋。

Q14. PREVENT/ASM如何優先處理企業需求（包括報告）？

客戶可以使用進階篩選選項，從企業角度決定基礎架構最重要的部分是什麼。

它會提供了關鍵風險指標，例如恢復時間和攻擊面發現的高風險漏洞數。另外可通過將資產和風險列表導出生成用於特定使用案例的報告。

Q15. 當PREVENT/ASM辨別出風險時，下一步是什麼？

傳統上，一旦檢測到漏洞或錯誤配置，人員需要手動處理風險。然而Darktrace PREVENT將提供高階風險面的能見度和相關的緩解建議來爲資安團隊提供進一步的幫助。

對於已部署Darktrace DETECT和Darktrace RESPOND的客戶，PREVENT/ASM的輸出可以作爲輸入，爲資安團隊提供更多時間解決問題。此方案是透過降低Darktrace PREVENT所標記易受攻擊的資產的檢測和警告標準，用一個安全網圍繞它們。當然，這取決於覆蓋區域的允許並啟用Darktrace RESPOND進入Active Mode。

產品部署

Q16. PREVENT/ASM如何部署？

PREVENT/ASM是一種雲端託管的SaaS產品，不需要客戶或終端用戶的輸入（這是零觸控）。簡單地說，只需要輸入使用品牌名稱，人工智能就可以從攻擊者的角度尋找在線上的品牌（這是零範圍）。

Q17. 如果一家企業擁有多個品牌怎麼辦？

客戶可以通過customer support要求將特定的資產或品牌添加到他們的環境中。

Q18. 我公司的名稱很常見，且其他公司也在使用，這樣PREVENT/ASM如何避免掃描到他們的IT系統？

PREVENT/Attack Surface Management除了使用公司名稱（例如使用他們的徽標等）之外，還使用其他信號來區分他們的品牌與其他公司。

Q19. PREVENT/ASM有不同的覆蓋範圍嗎？

沒有。PREVENT/ASM將覆蓋所有面向外部網路的資產、設備或環境（包括IoT、伺服器、DNS等）。

Q20. PREVENT/ASM可以多快完成設置？

5分鐘，不過需要一週的學習期。

Q21. PREVENT/ASM可以多快產生價值？

可立即產生價值，不過在開始進行深度挖掘之前，需要等待7天以確保獲得最完整的資訊。

Q22. 客戶可以使用PREVENT/ASM調查不屬於他們自己的組織嗎？

不行，他們只能調查自己組織的資料。

產品整合

Q23.與PREVENT/ASM有效運作需進行哪些項目整合？現有的Darktrace客戶是否能受益？

企業可以選擇在不購買任何其他產品或覆蓋範圍的情況下部署PREVENT/ASM。這些客戶可以從自動化的playbook、第三方整合或手動來解決檢測出的報告問題。

對於除了PREVENT/ASM之外還部署DETECT和RESPOND的客戶，產品價值會倍數增長。這些客戶可以從完整的Cyber AI Loop中受益，即一個產品的輸出作爲下一個產品的輸入，從而加強整個系統。這些客戶可以從Cyber AI Analyst的自動化報告和調查以及我們的自主反應能力（若已授權）中受益。

Q24. PREVENT/ASM與其他Darktrace產品如何配合（是否會淘汰其他產品）？

組織可以選擇部署PREVENT/ASM作爲獨立產品，或與DETECT或DETECT+RESPOND一同部署。Darktrace PREVENT旨在幫助防禦者預測網路攻擊，讓攻擊者在攻擊發動前更加困難（相比Darktrace DETECT和RESPOND則是應對已發動的攻擊）。PREVENT會向Darktrace DETECT和Darktrace RESPOND提供資訊，例如：

- 預防性地警告Darktrace / Email惡意域名正在冒充組織。
- 增強了端點和網絡層的檢測和響應機制。

資安分析師現在也可以利用外部數據加強調查，而Darktrace DETECT和Darktrace RESPOND創建的輸出也反饋到PREVENT。它們會形成一個不斷增強和學習的反饋「循環」。

產品部署

Q25. PREVENT/ASM與其他相關供應商產品有何不同之處？

許多供應商提供尋找威脅並識別已知漏洞（如Nessus by Tenable的漏洞掃描器）和攻擊面掃描（如網路設備的搜索引擎Shodan等）的解決方案。這些其他解決方案處理已知的已知威脅和已知的未知威脅。

Darktrace PREVENT/ASM使用人工智慧來理解什麼使外部資產屬於您的。

我們採用品牌爲中心的方法，聚焦於使您的品牌的獨特因素，然後利用這些特徵來識別構成你攻擊面的所有網路資產。我們的PREVENT/ASM爲「零範圍」和「零接觸」，因爲我們只使用您的品牌名稱來建立您的攻擊面。

雖然只需要品牌名稱即可開始搜索，但搜索範圍遠不止於此。它從數百個訊息源中提取資訊（超出已知的伺服器、網絡或IP地址）。例如，它可以使用語言識別和字符串解析算法來識別與品牌獨特的資訊所匹配的資產，以及分析與您的組織有關的網路應用程式。

Q26. Darktrace ASM能否能發現雲端應用程式?OT和IoT?APIs呢？

可以。Darktrace PREVENT/ASM可以發現那些與你的核心基礎設施具有技術關聯的資產（例如主域名、網路位址區塊等），或者根據公開可得的資訊（域名、註冊資訊、網站內容等）與你的品牌相關聯的資產。
值得注意的是，OT環境通常會希望被分區或隔離的（不連網）。因此，雖然暴露的OT資產很少見，但非常重要。

Contact Us

黃靖怡
台灣區業務總監

+886 972 600 229
+886 2 8729 5865

april.huang@darktrace.com
https://darktrace.com

臺北南山廣場
110臺北市信義區松仁路100號34樓

DARKTRACE