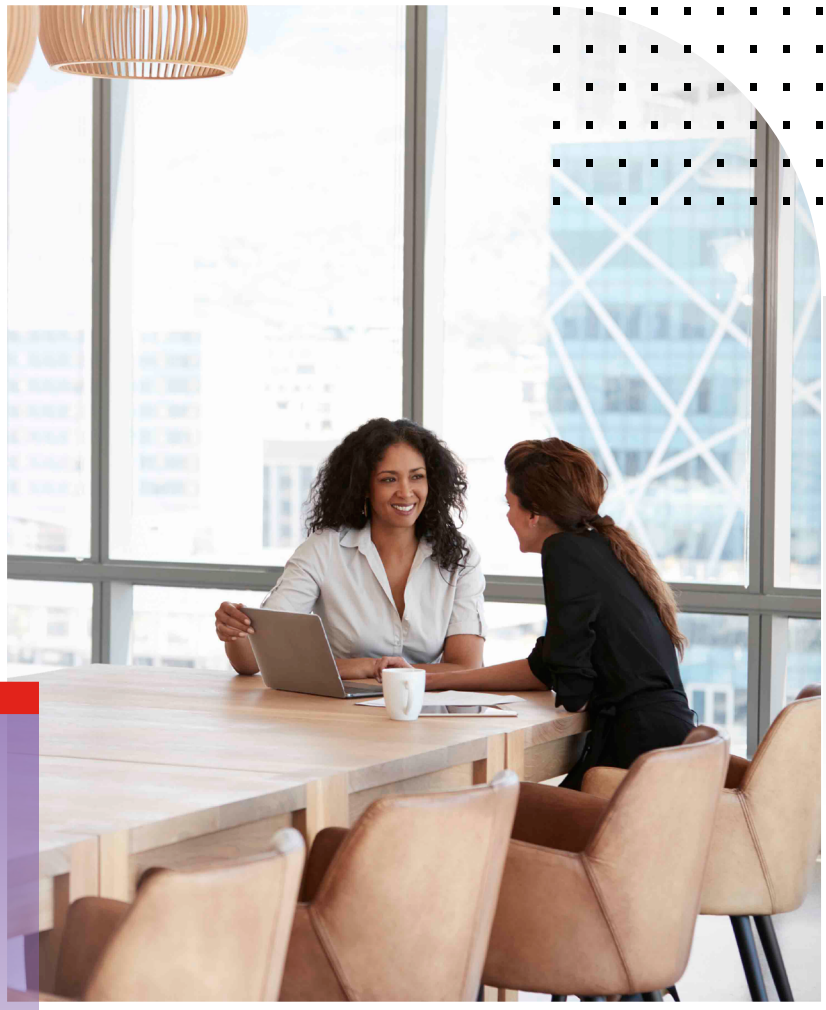
白皮書

評估端點安全解決方案

利用 MITRE Engenuity ATT&CK 資安框架進一步地了解端點安全的能力



內容提要

要選擇端點安全工具有時候並不容易，所以客觀中立的評比是重要的參考指標。

Mitre Corporation 是一家美國非營利組織，該組織在 2015 年 5 月發起 ATT&CK 資安框架研究計畫，整合了相關資安溝通語言，讓所有資安訊息可以統一辨識，加速判斷惡意行為的入侵方式，並且以更技術性的角度去評比產品的防禦能力，這也使得 Mitre 的資安防護評測成為了業界重要的參考指標。

企業可以利用 MITRE Engenuity ATT&CK 評測來得知各種端點解決方案的防護效能，並且透過使用 MITRE 工具來比較評估現有的檢測覆蓋率和漏洞，更可將結果與 MITRE 在現實世界攻擊中使用的大量戰術和技術進行比較，從而了解目前的安全狀況。端點安全的核心任務是降低資安風險，因此在評測解決方案之前，資安人員需要確保本身已經具備基礎的資安知識，資訊的最佳實踐可以顯著降低企業對資安威脅的暴險，安全專業人員應該有一個改善他們的安全態勢和可視性的策略。一旦具備了這些基本條件，就可以利用第三方評測來選擇最適合的解決方案。

當企業被問到在未來12-18個月最大的端點安全投資重點時，端點檢測和回應（EDR）產品是最常提到的優先事項。[1]

客觀的產品比較

今天多樣化的新型態攻擊和嶄新的網路威脅為不斷演變的資安威脅展開了新的局面。因此，企業的安全狀態與它賴以建立的各個安全控制至關重要。許多資安產品因為採取的方法或使用的術語不同，要對產品進行公平的測試比較並不容易，所以，當資安語言得到統一之後，溝通變得暢通，我們就可以清晰地了解各個產品的差異，並透過公平的評比來得知產品優劣，讓我們可以做出更明智的選擇，找到適合當前情況和所需要的資安解決方案了。

當然，因測試採用“黑箱”方式進行，所能得到的結果（阻擋或遺漏、已偵測或未偵測），而非實際在整體的資安構上顯示所有的資安機制運行，因此這樣的方式來判定測試的價值是相當具有挑戰性的。

MITRE ATT&CK Evaluations

從 2019 年開始，MITRE 即透過模擬真實世界，對端點安全解決方案的防護能力進行客觀和詳細的評測。MITRE 的模擬環境來自於公共網路的威脅情資報告，將其對應到 ATT&CK 技術知識庫，用複製行為的方法，對產品的效能進行客觀的評測。這樣的測試不僅顯示解決方案檢測特定活動的技術能力，更重要的是呈現許多當今網路威脅中常見的技術和戰術。

MITRE-Engenuity ATT&CK 評測方法非常強大，這個 ATT&CK 提供的框架，已經整合了現今大型駭客組織所使用的攻擊戰略與技術手法，並且以系統性的歸納方式，提供攻擊者對特定平臺（如：Windows）所採取的行動進行分類與分析，並整理成一個通用的模型。有別於以往在這一領域的測試方法，該測試的重點已不鎖定在對手所使用的工具和惡意軟體上，而是鎖定在操作期間如何與系統互動，而且，這個資安框架還在持續更新中。

為了提供測試環境，ATT&CK 資安框架透過技術組織成一套策略戰術。每一種技術都包含與維護者相關的資訊，以幫助他們了解使用中的技術所產生的事件和脈絡。使用的戰術和技術之間的關係可以在 ATT&CK 框架矩陣中看到，該矩陣涵蓋了 11 種不同的技術，並且為潛在的網路攻擊活動提供強大和細化的對應。每個區域有 10 種或以上的戰術，並透過持續的命令和控制來跨越初始存取。

2020 年的 ATT&CK 評估側重於模擬 Carbanak（一個針對銀行的駭客集團）和 FIN7（一個以財務為動機的駭客集團，它的主要目標為經常利用 POS 系統的惡意軟體，危害零售、餐飲和酒店業）。這些是優秀的測試範例，因為這些行業：

- 大量利用腳本、模糊處理、隱藏在可見位置的惡意軟體以及對機器後面的使用者進行攻擊。
- 使用多種獨特的操作工具，涵蓋複雜的意軟體以及能够與不同平台互動的合法管理工具。

2020 年，MITRE 擴大了測試範圍，包含了檢測結果與保護結果。除了測試技術或戰術是否能夠在某一點上被阻止之外，關鍵的區別在於，一旦這種戰術被阻止，就不可能對後期活動進行進一步的檢測。

檢測測試

對於檢測測試，評測涵蓋了 20 個測試範例。每個測試範例有多個階段。評測方式使用了六個術語來表達產品在每個測試中的表現，並指出了檢測的資料來源。

- **不適用（Not Applicable）**
  如果廠商沒有在測試系統上部署感測器，則使用此項。
- **無偵測（None）**
  在產品內無法看到檢測到測試行為的資料。
- **遙測（Telemetry）**
  可以看到這種行為，但只進行了最低限度的處理。
- **一般（General）**
  行為被處理和標記，但沒有詳細說明為什麼（戰術）或如何（技術）執行該行動。
- **戰術（Tactic）**
  行為被處理並被指定為惡意行為，同時還利用戰技或是其它關於網路攻擊的原因來豐富其內容。
- **技術（Technique）**
  該行為被處理並被指定為惡意行為，並以技術或其他關於它是如何被網路攻擊執行的方式來豐富其內容。

在檢測測試中，技術或戰術被標記為不適用（Not Applicable）的情況下，最好了解原因。這可能表示缺乏部署所需的作業系統或類似支援，或者，可能產品在設計上不是用來識別這樣的測試行為，當然也有可能還有其他原因，但其重要性需由使用單位來判斷。

在被測試的行為通常與潛在的合法操作以及惡意操作相關聯的情況下，無偵測（None）可能不是負面結果，尤其是如果讓該行為透過的風險是無害的。其中有個例子就是駭客還沒有達到他們的想要的結果。

遙測（Telemetry）與一般（General）的狀態則屬於第一級的檢測，可以在產品中識別並記錄行為，但對其識別原因的資訊有限。對於那些缺乏時間或專業知識的企業來說，這個級別足以深入了解網路駭客到底是如何執行任務的。對於那些想了解網路駭客詳細活動的資深資安人員來說，被標記為 MITRE 戰術或技術等級的檢測是最有價值。

測驗保護

保護測試只使用三個術語。

- **不適用（Not applicable）**
  該術語與檢測試驗中的術語相同。或者表示測試案例在檢測其餘的技術之前就被封鎖了。
- **無偵測（None）**
  沒有證據表明該技術因為該產品而受阻或不成功。
- **封鎖（Blocked）**
  技術被封鎖，並通知用戶它不成功。

雖然術語較少，但解釋起來比較複雜，因為封鎖的時間很重要，會根據測試案例的不同而變化。檢測誤報不在評測範圍內，但要考慮到，太早封鎖可能會增加誤報的可能性。相反，太晚封鎖可能使企業面臨一定程度的風險。下面是每種情況的案例。

假設測試 1 在第一步 1.a.1 被封鎖。這個結果似乎聽起來很棒，網路攻擊在最早期階段就被制止了。但是，如果實際上是執行工作的用戶被阻止了呢？在這種情況下，你會想知道用戶被阻止存取這個檔案的依據，是否有一個高可信度的惡意指標，或者存取政策設置得太過嚴格？或者，假設封鎖發生在步驟 2.b.5 的最後，也就是透過命令和控制通道進行的滲透。在這種情況下，該產品阻止了預期的資料洩露，但它確實允許發生步驟 2.b.1 遠端檔複製的生，這意味著該攻擊具有惡意影響。

在這種特殊情況下，考慮到收集到的 " 證據 " 和預期行動的惡意影響，證明阻止攻擊最安全時間點是第 1.a.3 步驟，且可以將誤報的風險降到最低。此步驟發生於當腳本程式嘗試第一次惡意檔案操作時，但這一資訊只有在了解每個階段的每個步驟和子步驟之後才能確定。成功或失敗是基於一個企業對誤擋合法用戶的活動與網路攻擊的所造成影響兩者孰輕孰重的考量和取捨。

Fortinet 正在參與 MITRE 2020 年的 ATT&CK 評測，該評測主要針對 Carbanak+FIN7 行為威脅者。

關於評測結果的重要提示

MITRE 強調，評測不是競爭分析，沒有分數、排名、評級或“贏家”，而是透過 ATT&CK 的語言和框架顯示觀察到的檢測結果以及每個廠商如何處理威脅檢測。這些評測可以幫助企業回答以下問題：

- 這個工具是否能檢測到你的組織中的已知威脅？
- 該工具如何將資料呈現給分析人員？
- 它能否在積極的檢測 / 保護和潛在的妥協風險之間取得平衡？

這個評測可以告訴你哪些廠商提供了跨越對手技術的最清晰的可視性，以及哪些廠商最能夠解決網路威脅所使用技術。評測可以呈現你可以獲得的見解，以及一個解決方案多久更新一次以涵蓋新對手所使用的技術。評測還可以告訴你，一個工具是否使用圖形化使用者介面（GUI），或為經驗較少的資安人員提供立即可使用的方式（turnkey），或提供更有經驗的資安人員可能需要的原始資料。

但是，評測無法回答以下問題：

- 對系統和使用者有什麼影響？
- 告警的數量以及所需的人工研究和調查的數量是多少？
- 該工具如何在你更廣泛的安全態勢中發揮作用？該工具是補充用的還是重複使用的？
- 系統是否錯誤地阻止了合法的行動？
- 所使用的工具如何與你的其他工具整合？
- 該工具的成本是多少？

要回答這樣的問題，需要進行額外的研究、測試，並考慮企業針對資安領域的長遠規劃。

評測的收穫

MITRE 測試的最大價值在於，它展示了一個產品抵禦由攻擊樣本所代表但不限於攻擊樣本的戰術和技術的能力。利用評測，你可以根據它的戰術和技術來測試你對以前未知攻擊的暴露程度，而不是基於現有的一對一或一對多威脅情資或模型。

CISO 可以使用 MITRE Engenuity ATT&CK 評測的結果來評測安全覆蓋範圍的差距。沒有單一的解決方案可以檢測到可能存在的每一種攻擊或技術，但你可以了解哪些產品可以檢測特定類型的攻擊。企業需要一個綜合的方法，以便能夠：

- 盡可能在攻擊的早期檢測和阻止威脅。
- 採取封鎖前平衡攻擊事件可信度 VS 提前封鎖。
- 找出包含威脅的解決方案。它是即時阻止惡意行為並使用微遏制（micro containment）和行程隔離（process isolation）來消除它們，還是依靠網路隔離來防止橫向移動？
- 在適當的情況下保留 " 強硬 " 的遏制工具，如行程終止（process termination）和端點隔離。
- 安全操作的簡化。

保留視角

端點安全比以往任何時候都更加重要。像勒索軟體這樣能夠快速移動的攻擊可以在幾分鐘內，甚至幾秒鐘內造成破壞。第一代 EDR 工具中的手動回應已經不敷使用。一個強大的網路安全基礎架構 (包括端點安全) 的目標是減少整體風險的暴露。有效的資安政策和持續的監測需要到位，以發現和預測、預防、檢測和回應，及補救攻擊。

發現、強化和預防是資安防禦的基礎。正確地做到這些基礎工作可以顯著降低風險。然而，每個 CISO 都會同意，儘管預防是不可或缺的，但預防永遠達不到 100%。

因此，除了預防之外，企業還需要有能力及早有效發現威脅，迅速回應和遏制威脅的入侵並恢復到已知的良好狀態。最終，目標是最大限度地減少業務的中斷，確保企業永續經營。

MITRE ATT&CK 評測可以幫助企業評測端點安全解決方案，其依據是最新的保護測試的檢測功效和某種程度的預防。然而，在選擇端點安全產品來滿足需求時，除了看 MITRE 的結果外，企業還應該：

- 透過發現和預測來實踐良好的資安環境，透過可見性和先發制人的控制來減少攻擊面，直到程式可以修補完成。
- 提高準確性，減少誤報和警報疲勞的影響。
- 注重反應，用精確和自動的回應將影響降到最低，以更有效地緩解風險。
- 即使在攻擊中也能保持系統的可用性和穩定性，特別是對操作技術（OT）和執行系統（executive systems）。
- 充分發揮技術的潛力；沒有任何工具會自行部署、運作和維護。

結論

MITRE ATT&CK 評測不僅僅是簡單的安全產品的有效性評分，而且更探索其操作方式。這種方法的主要好處是更好了解你所部署產品的各項反應能力。結合其他評測，您可以超越測試的特定範本，得到更多測試結果。MITRE ATT&CK 評測是一個很好的資源，可以幫助選擇端點安全產品，降低您最關注領域的網路安全風險，同時平衡，人、行程和系統的影響。評測還可以幫助你確定一個解決方案是否適合你的整體安全基礎架構。

然而，雖然某些攻擊不能單獨在端點中檢測到，但任何安全解決方案都不應該存在於真空中。同時，雖然重疊的覆蓋面比安全漏洞要好，某些行為可以透過多個解決方案來識別，但缺乏整合也會造成自身的挑戰。

[1] David Gruber, "ESG Master Survey Results: Trends in Endpoint Security," ESG, March 5, 2020.

www.fortinet.com/tw

June 14, 2021 8:24 PM
968201-0-0-TW