WHITE PAPER

Bitdefender®

MITRE ATT&CK® 2022 評測結果 — 解碼(硬核篇)

2022年3月31日，最新一輪MITRE ATT&CK®安全解決方案評估結果出爐。今年，包括Bitdefender在內領先的網路安全公司之30款安全解決方案接受了檢測Wizard Spider和Sandworm Team戰術(Tactics)和技術(Techniques)的能力測試。

第4輪MITRE評估側重於數據加密攻擊(Ransomware)(T1486)。攻擊者可能會加密目標系統或網路中大量系統上的數據，以中斷系統和網路資源的可用性。以Ryuk(S0446)和Conti(S0575)惡意軟體而聞名的Wizard Spider被選中代表勒索軟體行業。以NotPetya惡意軟體(S0368)聞名的Sandworm團隊代表了一種更險惡的軟體，旨在造成不可逆轉的破壞。兩者都是可以反應時勢的選擇——Conti勒索軟體在最近一次洩漏後受到安全研究人員的詳細審查，而像NotPetya這樣的資料加密軟體則被廣泛的部署在烏克蘭戰爭中。

是什麼讓MITRE ATT&CK®評估獨特而具有價值？

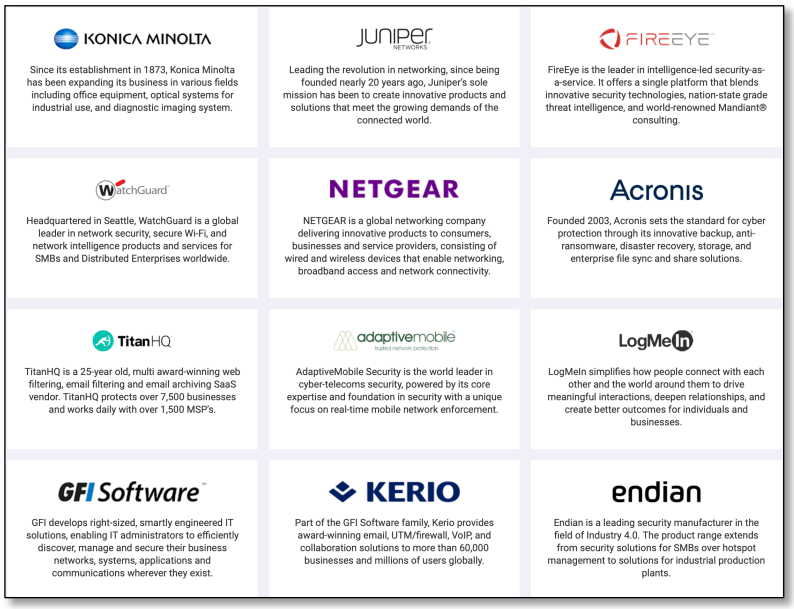
在充斥著過度宣傳的市場中，通過獨立的第三方測試驗證功能至關重要。AV-Comparatives和AV-TEST是評估安全解決方案的一些知名組織，MITRE Engenuity ATT&CK®評估在安全供應商和從業者中越來越受歡迎。

ATT&CK®評估在許多方面都是獨一無二的。MITRE不是測試解決方案阻止網路威脅的能力，而是模擬入侵者在通過層層預防機制後，所執行的的複雜完整行為。為達成此一目標，本次測試所有參加廠商均已關閉所有阻止或預防的功能，以便評估可以專注於檢測(Detection)、遙測(Telemetry)和分析(Analytics)的能力。

要理解ATT&CK®評估結果具有一定的挑戰性，因為MITRE Engenuity不發布比較分析，而是將其留給個人進行評估。評測的結果沒有分數、排名或評級。相反，評估顯示每個供應商如何在ATT&CK®知識庫的背景下處理威脅檢測。MITRE評估的結果非常廣泛，並且沒有競爭性排名，各種可能的解釋往往讓結果難以深入理解。Forrester分析師在博客“Winning” MITRE ATT&CK, Losing Sight Of Customer中很好地總結了如何正確使用ATT&CK評估的挑戰。

所有ATT&CK評估參與者的最終競爭對手都是入侵者。ATT&CK評估幫助安全供應商從這些練習中學習並改進其產品。**關於Bitdefender，我們感到非常自豪的是超過三分之一的參與供應商，購買或OEM至少一項的Bitdefender技術，從而證明了我們技術和專業知識的價值。**

Bitdefender OEM Technology Partnerships



資料來源：https://www.bitdefender.com/oem/technology-partnerships.html

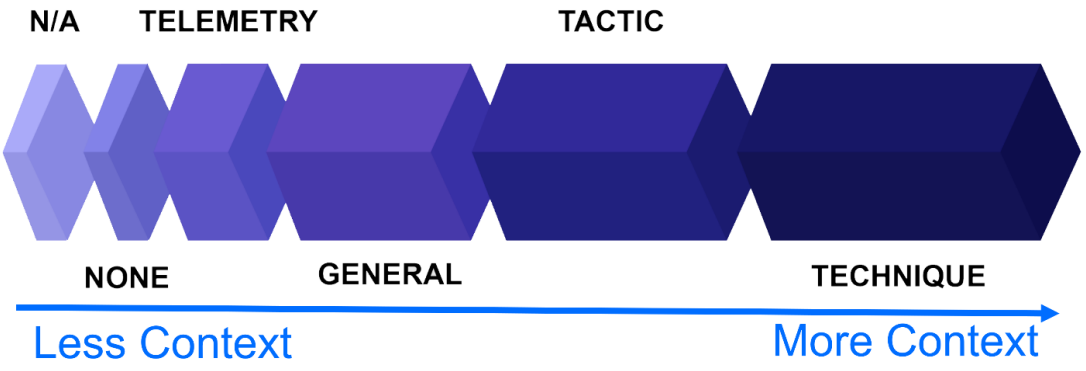
如何評價檢測質量？

缺乏競爭力的排名是ATT&CK®評估的一個與眾不同的特徵，但它不應該阻止資安社群花時間了解結果。評測結果為我們提供了極好的來源，以了解受測產品的偵測行為，並可作為其他獨立第三方報告的補充資料。

今年的ATT&CK®評估場景包含109個子步驟，涵蓋了廣泛的ATT&CK®戰術(Tactics)和技術(Techniques)。可視化當前一輪ATT&CK®評估中包含的戰術和技術的最簡單方法之一是使用ATT&CK® Navigator ——MITRE的一種基於網路的工具，用於可視化ATT&CK®矩陣。

ATT&CK® Navigator帶有用於當前一輪ATT&CK®評估的應用層。水平列代表戰術(Tactics)，垂直行代表技術(Techniques)，不同的顏色標識一個(或兩個)惡意組織使用的技術(Techniques)。
資料來源：*MITRE (上圖為本次評測專用的Navigator連結)*

對於每個子步驟，列出了達到的最高檢測類別。檢測類別告訴您安全解決方案是否具有查看行為的能力(遙測Telemetry)、是否具有分析能力來告訴您攻擊者試圖實現的目標(戰術Tactics)，或提供有關如何執行操作的詳細信息(技術Techniques)。



資料來源：麻省理工學院

MITRE提供了一些資源來幫助解釋結果，或者您可以**線上觀看Bitdefender網路研討會**2022 MITRE Engenuity ATT&CK®評估：解碼結果，來進一步解釋和理解2022年ATT&CK®評估結果。

Bitdefender結果

對於MITRE的每個子步驟，供應商都會收到以下「等級」之一。

- 無(None) - 未檢測到子步驟或低於最低要求的詳細信息
- 遙測(Telemetry) - 收集與子步驟相關的信息，但未解釋(僅原始數據)
- 一般(General) - 子步驟可疑，但沒有更多詳細信息可用。反惡意軟體檢測(沒有其他上下文)屬於此類別
- 戰術(Tactic) - 子步驟被識別為惡意。供應商知道發生了什麼，但不知道它是如何發生的。例如，檢測到從A到B的橫向移動，但不清楚威脅行為者如何在不同部分之間移動。
- 技術(Techniques) - 供應商了解它發生了什麼以及如何發生的。例如，檢測到從A到B的橫向移動，使用PsExec和從另一台機器竊取的憑據。

只有一般、戰術和技術等級計入分析覆蓋範圍。高分析覆蓋率代表受測產品不僅收集正確數據(可視性)，而且應用進階分析技術來準確關聯從不同傳感器收集到的事件。在我們自己的評估中，我們將「高」定義為覆蓋超過90%的子步驟。今年只有7家供應商達到了這一「高」分析覆蓋率的質量標準。

第四輪ATT&CK®評估確認Bitdefender的偵測結果具有高可行動性、在實現高效率資安監控和減少警報疲勞方面處於領先地位。

- Bitdefender在Windows機器上檢測到97%的所有主要攻擊步驟，以及100%針對Linux系統的入侵技術。
- Bitdefender GravityZone平台為109個子步驟中的106個 (97%)提供了分析，並為109個子步驟中的103個(95%)提供了技術級別描述(Techniques level)。

為了對這些結果進行比較，其他供應商的平均分析覆蓋率為71%，而技術級描述的平均覆蓋率僅為65%。

2022年4月4日更新：

我們的一些客戶和合作夥伴詢問了網上流傳的 “Results overview: 2022 MITRE ATT&CK Evaluation – Wizard Spider and Sandworm edition：總體檢測和保護” 圖表。

		Detection Rate	Prevention Rate	Total Rating
1	SentinelOne	99.08%	89.91%	94.50%
2	cybereason	100%	87.16%	93.58%
3	paloalto	98.17%	88.99%	93.58%
4	Cynet	98.17%	88.07%	93.12%
5	CROWDSTRIKE	96.33%	84.40%	90.37%
6	Microsoft	89.91%	85.32%	87.61%
7	TREND MICRO	96.33%	71.56%	83.94%
8	Malwarebytes	92.22%	67.89%	80.06%
9	McAfee	98.17%	59.63%	78.90%
10	FORTINET	96.67%	60.55%	78.61%
11	CYLANCE	81.65%	75.23%	78.44%
12	AhnLab	92.22%	61.47%	76.85%
13	cisco	82.57%	67.89%	75.23%
14	Check Point	94.50%	55.96%	75.23%
15	FIREEYE	81.65%	55.05%	68.35%

		Detection Rate	Prevention Rate	Total Rating
16	vmware Carbon Black	82.57%	50.46%	66.51%
17	Symantec	84.40%	47.71%	66.06%
18	SOPHOS	80.73%	44.95%	62.84%
19	eset	83.33%	33.94%	58.64%
20	deep instinct	70.00%	46.79%	58.39%
21	CYCRAFT	70.64%	39.45%	55.05%
22	Bitdefender	97.25%	0%	48.62%
23	elastic	89.91%	0%	44.95%
24	Uptycs	84.40%	3.67%	44.04%
25	Fidelis	86.24%	0%	43.12%
26	REAQTA	78.89%	0%	39.44%
27	F-Secure	76.15%	0%	38.07%
28		75.56%	0%	37.78%
29	Qualys.	73.33%	0%	36.67%
30	RAPID7	56.88%	0%	28.44%

每年在發表評測結果後，一些供應商在解釋MITRE和其他評估的結果時，都會使用誤導性的行銷做法。ATT&CK評估的主要價值在於提供對不同安全解決方案的檢測和分析能力的洞察。Prevention評測是ATT&CK的補充項目，供應商可選擇是否參與。

不幸的是，許多供應商今年決定將他們的行銷重點，放在這些非必要性的的評測項目上，並誤導性地將不參加此測試項目的供應商包括在內，並將這些供應商的在該項目的 “得分” 設定為為零。事實上， 由於發佈者無法驗證數據的準確性，這篇關於Help Net Security的廣為流傳的文章已被刪除。

1. 參與者付費參與ATT&CK評估——“Protection”評估需要供應商額外付費。包括Bitdefender在內的許多供應商選擇退出此Protection評測，因為市場上已有為數不少的Protection獨立專門評測。我們得出的結論是，額外的成本和努力不會為我們的 Bitdefender Labs團隊提供重要的研究價值，因為我們在最近幾個月和幾年中使用AV-Comparatives和AV-TEST進行了許多此類測試。MITRE ATT&CK測試中保護測試的Bitdefender分數不是0，而是「不適用 (N/A)」。為了將我們的解決方案與其他供應商進行比較，我們建議在AV-Comparatives或AV-TEST等網站上進行獨立比較。

2. 注意改寫或誤導MITRE術語原意的供應商。MITRE用詞中的「檢測率(Detection Rate)」或「總體檢測(Overall Detection)」指的的是MITRE稱為「可視性(Visibility)」的指標。可視性是Low-context(遙測-原始數據)和High-context(了解發生了什麼以及如何發生)的組合。高可視性意味著安全供應商收集了正確的數據，但沒有說明分析能力、幫助緩解警報疲勞的能力，並且容易出現更多誤報。當供應商決定用委婉語來替換MITRE名詞時(例如將「遙測」重命名為「提供證據」)，我們建議將其視為一個警告信號。

CISO和安全團隊如何解讀結果？

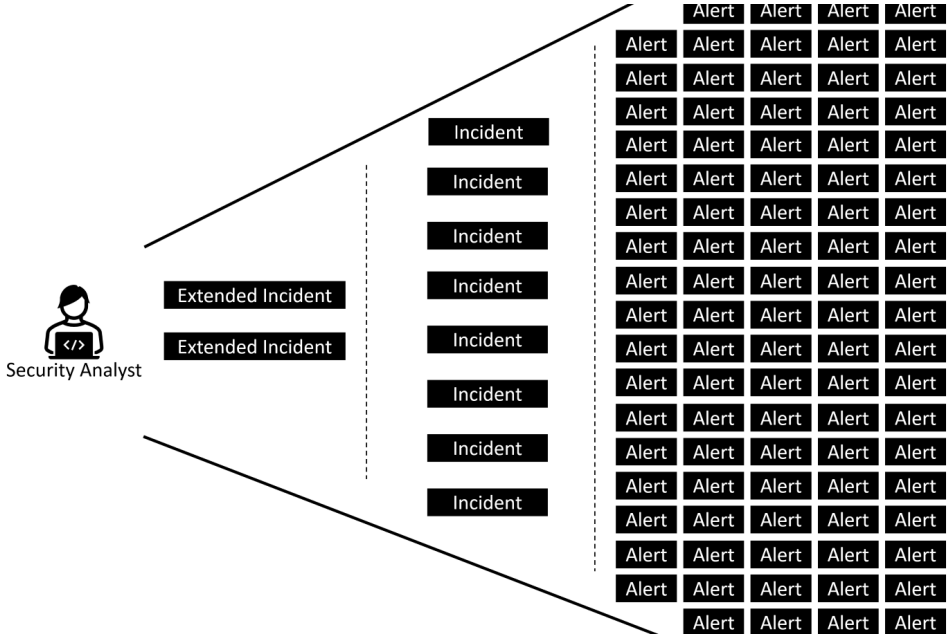
在評估此數據時，我們建議首先了解您的需求，並評估在當前威脅形勢下，您的組織最需要的技術。此方式可以幫助識別您當前部署的安全機制和重要監控指標間二者的差距。為了有效實施ATT&CK®框架，我們還建議根據您的業務優先需求來對其進行調適。Gartner在這篇博客文MITRE ATT&CK中分享了他們收到的一些常見詢問和ATT&CK框架領先實踐-是嗎？你需要它做什麼？，您可能會覺得很有幫助。

端點檢測和響應(EDR)和擴展檢測和響應(XDR)解決方案的基本價值，是最大限度地減少入侵者的停留時間。ATT&CK®評測旨在描述供應商是否能收集正確的數據(遙測)，來正確識別入侵行為的戰術(Tactics)與技術(Techniques)步驟，並對其提供分析的能力。

在考慮安全解決方案時，ATT&CK®評測結果是一種有價值的工具，但是它們不能替代POC(Proof Of Concept)。ATT&CK測試環境規模最小，評估不考慮成本、產生多少噪音(警報疲勞)或與安全解決方案操作相關的挑戰等因素。我們還建議將MITRE結果與其他專注於威脅預防的獨立第三方測試一起解釋，例如AV-Comparatives和AV-TEST。

在評估結果時，我們建議您自己得出結論，而不是僅僅依賴安全供應商**(甚至是我們的！)**的解釋。今年引入的變化之一是每個子步驟只能有一個檢測類別(None, General, Telemetry, Tactic, Techniques之一)，代表在該子步驟的所有檢測中可供分析的最高情境上下文。這是一個重要的變化，因為在某些類別中得分高不一定是一個正面的信號。例如，如果供應商的遙測覆蓋率很高，這可能意味著他們的分析能力無法有效使用遙測數據，從而讓該產品的分析覆蓋範圍有限。

要了解有關2022年MITRE Engenuity ATT&CK®評估報告中包含的關鍵指標的更多信息，請觀看我們於2022年4月6日舉行的實時網路研討會。Dragos Gavrilut是ATT&CK®評估的主要參與者之一，他將分享他對方法、關鍵指標以及如何使用結果來提高您的網路彈性的見解。



ATT&CK® 評估不涵蓋安全解決方案的運營方面。事件的自動關聯和整合的用戶體驗對於有效減少警報疲勞至關重要。

本文參考出處：
https://businessinsights.bitdefender.com/mitre-attck-evaluations-2022-why-actionable-detections-matter

Bitdefender®

www.bitdefender.com

Cyberview
力悅資訊

Bitdefender 臺灣區代理商 — 力悅資訊股份有限公司
臺北市中山區松江路54號4F-4 | 02-2542-9758 | Sales@cyberview.com.tw

Bitdefender is a global cybersecurity leader protecting over 500 million systems in more than 150 countries. Since 2001, Bitdefender innovation has consistently delivered award-winning security products and threat intelligence for the smart connected home, mobile users, modern businesses and their networks, devices, data centers and Cloud infrastructure. Today, Bitdefender is also the provider of choice, embedded in over 38% of the world's security solutions. Recognized by industry, respected by vendors and evangelized by customers, Bitdefender is the cybersecurity company you can trust and rely on.

Bitdefender-Business-WhitePaper-VSI-CREA3420-A4-en_EN