本所採用端點偵測與應變(EDR)及託管式偵測與應變(MDR)資安服務分析

運輸科技及資訊組　吳東凌 童志浩

研究期間112年2月至112年12月

摘　要

隨著網路安全威脅的日益增長和複雜化，組織面臨著前所未有的安全挑戰。在這樣的背景下，端點偵測與應變(Endpoint Detection and Response, EDR)和託管式偵測與應變服務(Managed Detection and Response, MDR)成為當前網路安全領域的重要組成部分。本文旨在探討EDR和MDR在現代資安架構中的角色、功能及彼此間的互動關係，並分析它們如何共同提升組織的安全防護能力，總結了EDR和MDR整合為組織帶來的價值，包括提高了威脅偵測和回應的效率、強化了組織的整體安全，以及如何幫助組織更好地應對日益複雜的安全挑戰。

關鍵詞：

端點偵測與應變(EDR)，託管式偵測與應變服務(MDR)，網路安全，威脅偵測，資安服務

一、緒論

(一)背景介紹

在數位化日趨普及的當今社會，資訊安全問題成為政府機構待解決的重大課題。近年來，資安威脅呈現快速演進的趨勢，給政府帶來了前所未有的挑戰和風險。隨著科技進步，網路攻擊手法不斷翻新，從最初的病毒、蠕蟲到今日的勒索軟體、惡意程式攻擊等，威脅不斷升級和變化。近年來隨著物聯網、雲端計算、大數據等技術的廣泛應用，資安威脅面臨更多元化和複雜化的挑戰。

資訊安全問題對組織和政府機構來說，不僅是技術層面的挑戰，更是涉及組織營運、資料保護、公眾信任等多個層面的綜合問題。資安事件不僅可能導致組織資料外洩、業務中斷，甚至可能對國家安全和社會穩定造成嚴重影響。因此，如何有效應對資安威脅，成為了組織和政府極需解決的核心問題。

在眾多的資安解決方案中，端點偵測與應變(Endpoint Detection and Response，簡稱 EDR)和託管式偵測與應變(Managed Detection and Response，簡稱 MDR)逐漸受到廣大組織的重視和採用。EDR 專注於端點設備的資安監控和應對，能夠即時偵測異常行為，提供即時警報和反應。其高度自動化和精確的偵測能力，使得組織能夠迅速識別和反應各種威脅，減少損失和風險；MDR 則提供了更為綜合和集中的資安服務，不僅包括端點偵測，還涵蓋網路、雲端、應用等多個環節。透過第三方專業團隊的支持，MDR 能夠提供更全面、深入的威脅狩獵和應對，協助組織建立更為強大和可靠的資安防禦體系。

二、端點偵測與應變(EDR)的技術與特性

(一)EDR的基本概念

隨著資訊科技的飛速發展，資訊安全成為組織和組織不可忽視的重點領域。端點偵測與應變是當前資安領域的核心技術之一，它對於識別、調查和應對資訊系統中的惡意活動至關重要。

EDR 是一種安全解決方案，旨在監控和反應組織網路中的端點(如電腦、移動設備等)所面臨的安全威脅。通過即時收集來自端點的數據，分析潛在的惡意活動，並提供必要的應對措施以防止威脅擴散。EDR 處理流程如圖二所示。

核心功能包括：

1. 即時監控與數據收集

EDR 系統能夠持續監控端點的行為和狀態，同時收集相關數據，如文件活動、網路通信和登錄行為等。

2. 威脅偵測與警報

通過分析收集到的數據，EDR 系統能夠識別異常行為和潛在的安全威脅，並對安全團隊發出警報。

3. 調查與反應

當偵測到潛在威脅時，EDR 允許安全人員進行深入調查，確定威脅的性質和範圍，並採取必要的應對措施。

在當今複雜的網路環境中，僅依靠傳統的病毒掃描和入侵檢測系統已不足以應對日益精密的網路攻擊。因為許多先進的威脅，如零時差攻擊(zero-day attacks)和持續性威脅(APT)，往往能夠繞過基於簽名的傳統安全措施(如圖一)。在這種情況下，行為分析成為了一種重要的防禦手段。行為分析通過監控和評估端點上的活動，如文件存取、應用程序行為和網路流量，來識別惡意或異常行為。這種方法的優勢在於能夠偵測到未知的或定制化的攻擊，從而為組織提供更全面的保護。

在當代的資安策略中，威脅情報的角色變得日益重要。威脅情報整合指的是收集、分析及分享有關現有或新興威脅的資訊，以便更有效地識別、評估和對抗網路攻擊。威脅情報整合的主要優勢包括：

1. 預警與預防

通過即時監控和分析全球資安威脅趨勢，組織能夠獲得先行警示，並採取措施防範潛在威脅。

2. 針對性的防護措施

威脅情報可協助組織了解特定攻擊者的行為模式、攻擊手法和目標，從而開發出更加精確有效的安全策略。

3. 資源優化

透過威脅情報，組織能夠更有效地分配資源，專注於最有可能面臨的威脅，而非廣泛、隨機的防範。

將威脅情報整合到 EDR 解決方案中，可以顯著提升安全防禦能力。透過對全球威脅情報的即時訪問和分析，EDR 系統不僅能夠識別已知威脅，還能夠預測和對抗新興的攻擊手段。這種整合不僅增強了偵測和反應的速度，還提高了整體安全架構的智能化和適應性。

EDR 的優勢：

1. 即時偵測與反應

EDR 系統最大的優勢之一是其即時監控和快速反應能力。與傳統的防病毒軟體相比，EDR 不僅能偵測已知的惡意軟體，還能識別未知或零時差攻擊。因為 EDR 專注於行為模式的分析，而不僅僅是病毒特徵碼的匹配。

2. 全面覆蓋與深入見解

EDR 提供了對組織所有端點的全面監控，從而實現了對潛在威脅的深入洞察。這些端點包括不僅限於辦公室內的電腦，還包括遠端工作員工的移動裝置和家用電腦，從而確保了組織在各種工作環境下的安全。

3. 適應性與學習能力

EDR 系統通常包括機器學習和人工智慧技術，這使得它們能夠隨著時間的推移不斷適應新的威脅模式。這種學習能力意味著 EDR 系統能夠隨著網路環境的變化而進化，提供更加精準的偵測和反應。

(二)EDR面臨的挑戰和解決方案

儘管 EDR 帶來了許多優勢，但在實際部署和運營過程中也面臨著一些挑戰：

1. 數據量和複雜性

隨著組織網路的擴張和複雜化，EDR 系統需要處理的數據量也在不斷增加。大量數據的分析和儲存對系統的性能提出了高要求。此外，大數據環境中的偽陽性和偽陰性問題也可能對系統的有效性造成影響。解決方案為：針對數據量和複雜性的挑戰，組織可以採用雲基礎的 EDR 解決方案，利用雲計算的可擴展性和彈性來處理龐大的數據。同時，進一步完善機器學習算法，提高偵測精準度，減少誤報率。

2. 技術專業性和操作複雜性

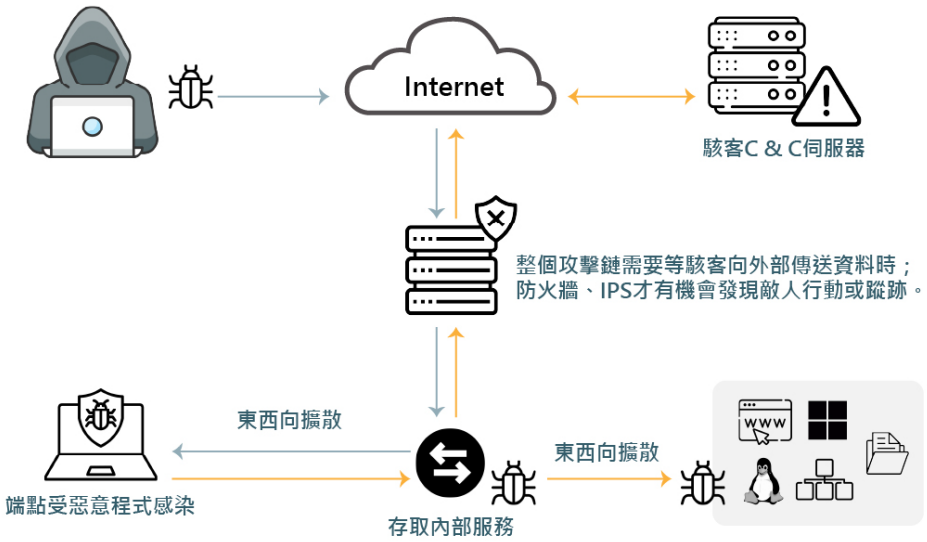
EDR 系統有效運營需要高水準的技術專業性和安全知識。許多組織可能缺乏足夠的專業人員來管理和調整 EDR 系統。解決方案為：組織可以考慮與專業的安全服務提供商合作，利用其專業知識和經驗來管理 EDR 系統。此外，培訓和提升內部團隊的技能也是一個有效的策略。

3. 操作性和整合問題

在多廠商環境下，EDR 系統與其他安全工具(如防火牆、入侵檢測

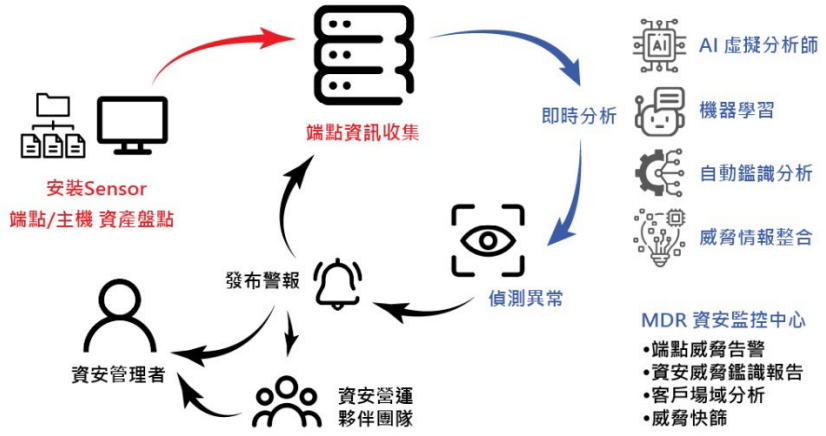
系統等)的互操作性成為一大挑戰。這可能導致安全盲點和效能下降。解決方案為：選擇支持開放標準和 API 的 EDR 解決方案，以便與現有的安全架構無縫整合。此外，進行定期的系統審核和測試，以確保所有元件協同工作，實現最佳的安全性能。

總結來說，EDR 系統為組織提供了一種高效的方式來應對不斷變化的網路威脅。通過即時的威脅偵測和反應、全面的端點覆蓋和智能的學習能力，EDR 提升了組織的整體安全態勢。然而，隨著這些系統面臨的挑戰，如數據管理、技術專業要求和系統整合問題，組織需要找到有效的解決方案來確



圖一、駭客攻擊模式

資料來源：仁大資訊(https://www.hpicorp.com.tw/solution-service/29f024b6-e0bb-11ec-b659-1e369c064646)



圖二、EDR 處理流程

資料來源：仁大資訊(https://www.hpicorp.com.tw/solution-service/29f024b6-e0bb-11ec-b659-1e369c064646)

三、託管式偵測與應變(MDR)的運作原理與特色

(一)MDR的基本概念

隨著網路安全威脅的日益增加和複雜化，組織正面臨著前所未有的安全挑戰。託管式偵測與應變(MDR)作為一種新型的資安服務，為組織提供了一個有效的解決方案來應對這些挑戰。MDR 是一種外包的安全服務，旨在幫助組織偵測、調查和應對網路威脅。與傳統的安全服務不同，MDR 提供更為主動和定制化的安全監控和威脅處理。這種服務結合了最新的安全技術、專業的安全分析師和快速應對機制，為組織提供 24 小時不間斷的全方位安全保護，MDR 服務流程如圖三，MDR 服務架構如圖四。

MDR 的核心功能如下：

1. 持續的威脅監控和偵測

   MDR 服務利用先進的技術和工具即時監控組織的網路系統偵測潛在的安全威脅。

2. 威脅情報和行為分析

   透過不斷更新的威脅情報和行為分析，MDR 能夠識別出複雜的攻擊模式，包括先進持續性威脅(APT)。

3. 快速的事件反應

   當偵測到威脅，MDR 團隊將迅速進行調查，並採取必要的應對措施，以減輕或消除威脅帶來的影響。

MDR 服務不僅對現有威脅的被動防禦，而是一種主動的安全策略。這種策略的關鍵在於三大核心要素的有效整合：

1. 監控

   持續監控是 MDR 的基石，它確保了對組織網路活動的全天候監視。這不僅包括檢測已知的威脅模式，還包括對異常行為的識別，這些異常行為往往預示著新型或未知的攻擊。

2. 狩獵

   威脅狩獵涉及主動搜索和識別尚未被自動化系統發現的威脅。此類方法依賴於安全專家的經驗和專業知識，他們使用先進的分析技術來深入組織網路，識別潛藏的威脅。

3. 應對

   當偵測到威脅，快速有效的應對是至關重要的。MDR 提供的應對措施包括隔離受影響的系統、刪除惡意軟體、修復漏洞以及提供事後修復建議。這種快速反應能力減少了威脅可能造成的損害。

在 MDR 模型中，第三方服務提供商扮演著關鍵角色。他們不僅提供技術和工具，而且還提供人力專業知識，這對於大多數組織來說是難以內部實現的。

1. 專業知識和經驗

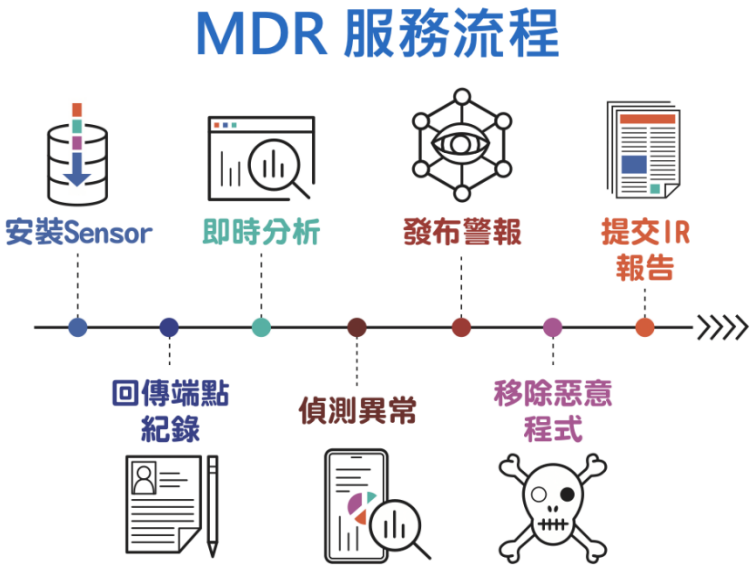
   MDR 提供商通常擁有一支由經驗豐富的安全專家組成的團隊。這些專家對最新的威脅趨勢有深入了解，能夠應對各種複雜的安全挑戰。

2. 持續的支持和咨詢

   除了提供監控和反應服務外，MDR 提供商還為客戶提供持續的安全咨詢和支持。這包括幫助組織建立和完善其整體安全戰略，以及提供培訓和意識提升活動。

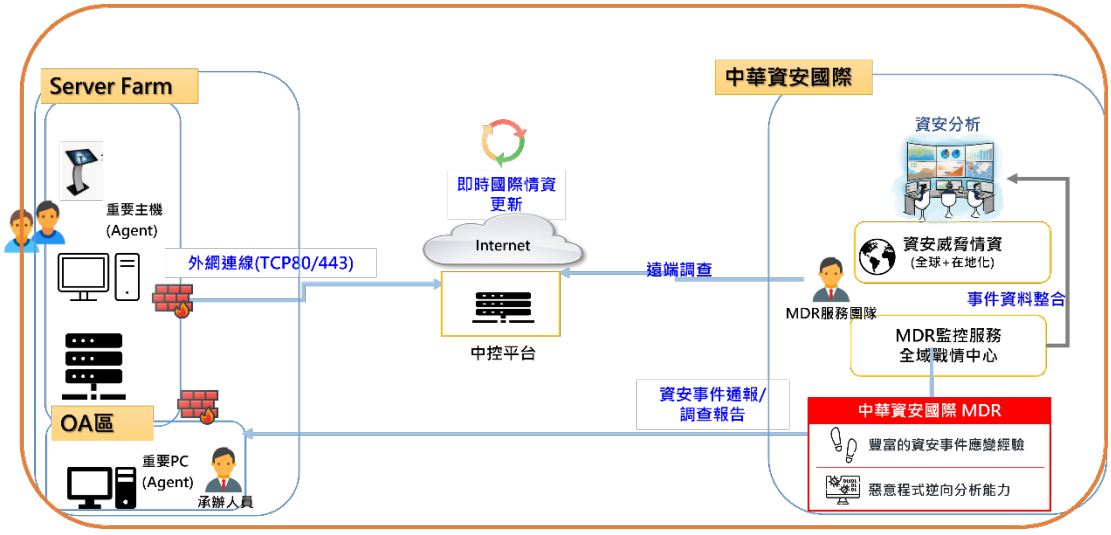
3. 定制化服務

   不同的組織有不同的安全需求。MDR 提供商通常能夠提供定制化的服務來滿足這些特定需求。這包括針對特定行業的安全標準和合規要求提供定制的解決方案。



圖三、MDR 服務流程

資料來源：天鈺科技(https://www.yottatech.com.tw/?q=node/74)



圖四、MDR 服務架構

資料來源：中華資安國際(https://www.chtsecurity.com/service/m305)

MDR 的優勢：

1. 增強的威脅偵測能力

   MDR 系統通過收集和分析端點數據(如文件活動、網路通信、用戶行為等)，能夠識別先進的、隱蔽的威脅，這些威脅可能被傳統的防毒軟體所忽略。

2. 外部專業支援

   由外部供應商提供的 MDR 服務，通常擁有豐富的經驗和專業知識，能夠迅速識別新興威脅，以及提供最佳的安全實踐。

3. 即時監控與快速回應

   MDR 提供 24 小時不間斷監控，能夠即時發現異常活動。在檢測到潛在威脅時，MDR 團隊能夠迅速回應，減少損害和數據損失。

4. 自動化與人工智慧

   MDR 服務通常整合了自動化和人工智慧技術，能夠自動處理常見的威脅，同時針對複雜的攻擊情境提供人工專業的介入。

5. 針對性調查和威脅狩獵

   MDR 不僅限於應對已知的威脅，還包括針對性的調查和威脅狩獵，以發現組織可能尚未察覺的高度進階的攻擊。

6. 適應性更新

   MDR 供應商會定期更新其威脅情報和安全措施，確保能夠應對新興威脅。這種適應性更新有助於保持組織的安全性。

7. 節省內部資源

對於資源有限的組織而言，MDR 的外包服務可減輕內部安全團隊的工作負擔，使其能夠專注於更戰略性的安全任務。

通過這些優勢，MDR 成為了現代組織安全架構中不可或缺的一部分，幫助組織更有效地對抗日益複雜和精細的網路威脅。

(二)MDR面臨的挑戰和解決方案

儘管 EDR 帶來了許多優勢，但在實際部署和運營過程中也面臨著一些挑戰：

1. 複雜的威脅環境

   威脅演進快速，攻擊方式不斷變化，讓檢測和防禦變得更加複雜。解決方案為：不斷更新威脅情報、使用先進的機器學習和人工智慧技術，以應對新型威脅。

2. 資源限制

   組織可能缺乏足夠的人力和資源來有效地實施和維護 MDR 服務。解決方案：利用外包的 MDR 服務，將安全監控和事件反應交由專業團隊，減輕組織自身的負擔。

3. 大量的虛擬環境和多雲環境

   當組織使用多種雲端提供商或組織擁有複雜的虛擬環境時，MDR 變得更加複雜。解決方案：提供支援各種環境的 MDR 服務，並整合安全解決方案以確保全面的覆蓋。

4. 威脅檢測與誤報問題

   高靈敏度的威脅檢測有可能導致誤報，增加管理負擔。解決方案：透過威脅情報的改進、調整檢測規則以減少誤報，並進行合理的事件分析。

5. 內部和外部協作

   在組織內部和外部(如供應鏈)協作可能受到限制，影響 MDR 的效力。解決方案：建立有效的溝通和合作機制，包括共享威脅情報，以迅速應對新的威脅。

6. 人力不足和技術技能不足

   安全領域的技術需求不斷變化，而找到具有相應技能的專業人才變得困難。解決方案：提供培訓、吸引和保留優秀的安全專業人才，或透過外包來獲得所需的技能。

四、EDR、MDR 整合

在當今逐漸複雜化的網路威脅環境中，組織安全體系的建立與強化成為迫切需求。在眾多安全解決方案中，端點偵測與應變(EDR)和託管式偵測與應變服務(MDR)的結合，正成為業界趨勢。本文旨在分析 EDR 與 MDR 整合的必要性、實施過程中的挑戰與機遇，以及這一趨勢對組織安全戰略的長遠影響。

(一)EDR與MDR差異

EDR 系統主要聚焦於端點安全，透過收集和分析終端設備上的數據，來識別、調查和回應安全威脅。相對的，MDR 提供更為廣泛的服務範疇，不僅包括威脅偵測和反應，還提供全天不間斷監控、事件分析與處理等服務。

(二)EDR與MDR整合的必要性

隨著網路攻擊手法的日益翻新，僅依賴 EDR 的端點保護已難以滿足組織全面安全需求。EDR 擅長捕捉端點異常行為，但在面對複雜多變的攻擊模式時，可能無法完全滿足偵測與回應的需求。MDR 的引入能夠彌補 EDR 的不足，提供更全面的安全保護。

整合可能面臨的挑戰：

1. 技術兼容性

   不同 EDR 和 MDR 解決方案之間的兼容性可能成為一大挑戰。整合過程中需確保兩者之間的無縫連接和數據共享。

2. 操作複雜性

   整合 EDR 和 MDR 可能會增加系統的操作複雜性，給安全團隊帶來新的管理挑戰。

3. 成本考量

   部署和維護 EDR 和 MDR 的整合系統可能會帶來額外的成本。

整合的優點：

1. 全方位威脅防禦

   整合 EDR 和 MDR 能夠為組織提供更全面的威脅偵測與回應能力，尤其在對抗先進持續性威脅(APT)方面。

2. 提升應對效率

   結合 MDR 的專業知識和 EDR 的技術能力，能夠加快威脅偵測與回應速度，降低安全事故的潛在影響。

3. 資源最優化

透過專業的 MDR 服務，組織可以將更多資源集中於核心業務，同時保持強大的安全防禦。

EDR 與 MDR 的整合不僅是技術層面的結合，更是一種安全思維的轉變。它要求組織在構建安全架構時，不僅要考慮技術層面的防禦，還要整合專業團隊的監控與反應能力，形成更為全面和深入的安全防禦體系

六、結論

隨著網路威脅的日益複雜多變，EDR 與 MDR 的整合趨勢正逐漸成為組織安全戰略中的一部分。這趨勢不僅提升了組織對抗網路威脅的能力，還促進了安全技術的進步與創新。組織需要認識到這一變化，並積極調整自身的安全戰略，以確保在這個不斷變化的網路環境中保持競爭力。對於需要專注於終端設備的安全監控和應對的組織來說，EDR 會是一個經濟實惠且有效的解決方案；而對於需要提升安全能力及整體安全解決方案，以增強組織內部資安防護能量的運研所而言，MDR 則更為合適。MDR 可提供更全面、更專業的安全服務，運研所只須定期透過供應商所提供的分析報告瞭解自身資安狀態，並依建議處理風險即可。

參考文獻

1. 蓋亞資訊：https://www.gaia.net/tc/news_detail/2/216
2. iT邦幫忙：Jhttps://ithelp.ithome.com.tw/articles/10307982?sc=iThelpR
3. 電腦科技電子報：https://www.syscom.com.tw/ePaper_New_Content.aspx?id=958&EPID=308&TableName=sgEPArticle
4. 資安趨勢部落格：https://blog.trendmicro.com.tw/?p=60557
5. 資安人：https://www.informationsecurity.com.tw/article/article_detail.aspx?aid=9558
6. 數位通國際：https://www.easpnet.com/blog/mdr-edr-services/
7. 網管人：https://www.netadmin.com.tw/netadmin/zh-tw/technology/61C38768F6C24CE8B03B169D0FBFEBBE
8. 趨勢科技：https://www.trendmicro.com/zh_tw/what-is/xdr/edr.html#edr-tm-id
9. 鼎新電腦：https://techops.digiwin.com/edr_protect/
10. 中華電信：https://secure365.hinet.net/EnterpriseSecurity/product/inner.do?product_id=489d58acf9000000ad2c04c81d9576fc
11. Freedom Systems：https://www.freedom.net.tw/ict-insight/security/mdr-vs-mssp.html
12. 蓋亞資訊：https://www.gaia.net/tc/news_detail/2/216