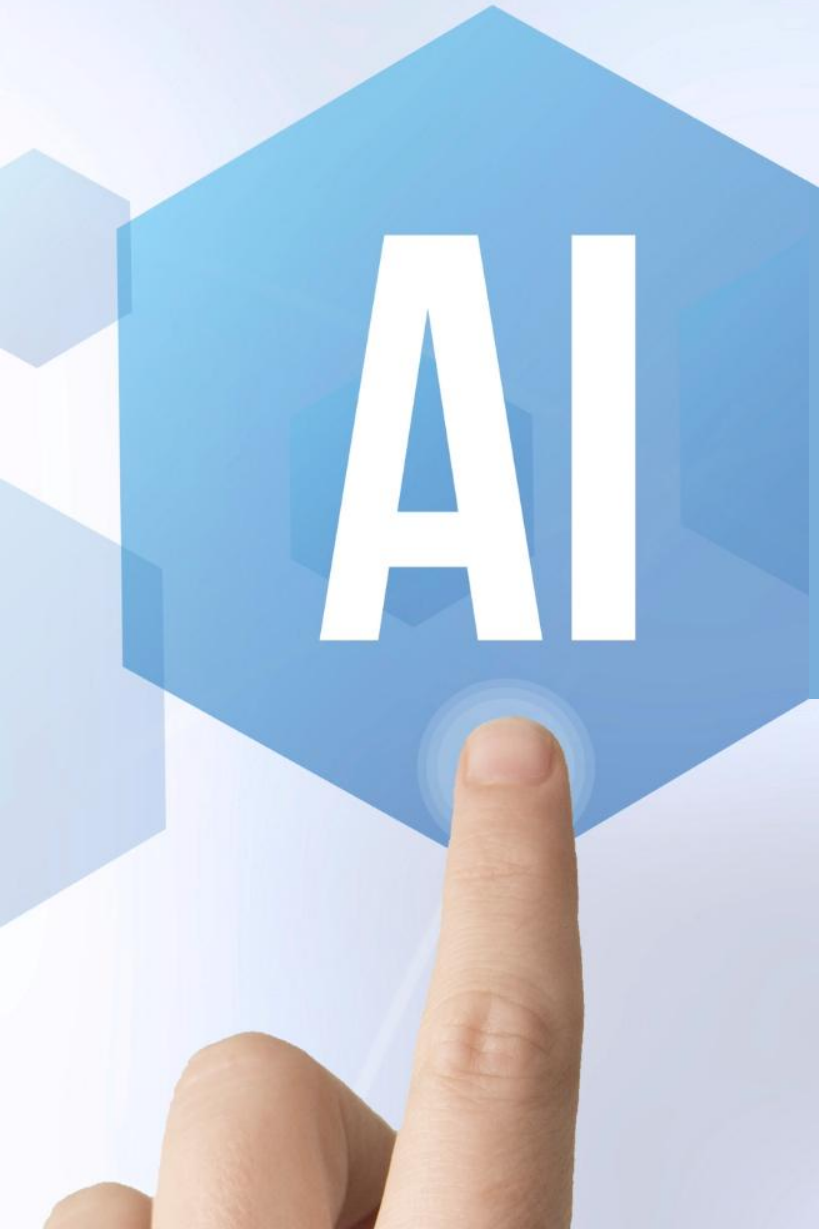
AEB 宏碁資訊

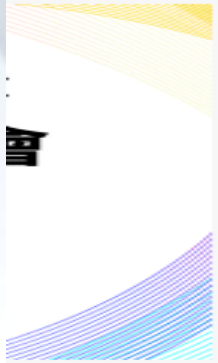


重灌人生太淒涼
來點不一樣的 MDR

Speaker : Joseph Liao

最懂地端的雲端公司 企業生成式AI加速器

MDR的效益



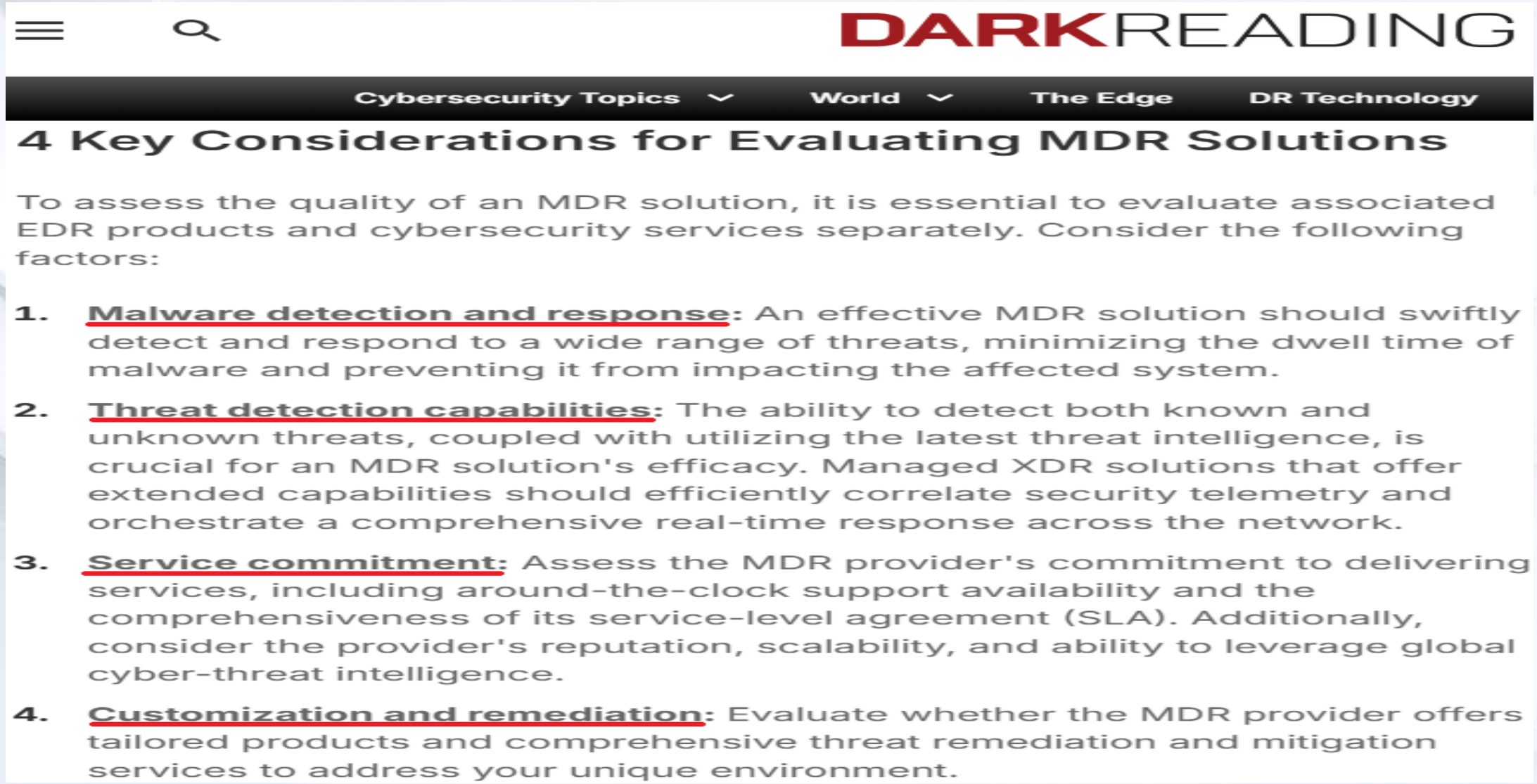
Sophos 委託進行的一項獨立研究，評估了各種網路安全防禦措施對網路保險理賠金額的財務影響，以及資安產品與服務的投資報酬率 (ROI)。研究結果顯示，在美國，使用託管式偵測與回應 (MDR) 服務的企業，其網路保險理賠金額比僅依賴端點防護的企業低 97.5%。

研究重點發現：

- MDR 服務顯著降低了理賠金額：使用 MDR 服務的企業，其理賠金額比僅依賴端點防護的企業少 97.5% (7.5 萬美元 vs. 300 萬美元)。
- EDR/XDR 解決方案亦可減少理賠金額：使用 EDR/XDR 的企業，其理賠金額僅為單純使用端點防護企業的六分之一 (50 萬美元 vs. 300 萬美元)。
- 使用 MDR 服務的企業理賠金額最具可預測性，而使用 EDR/XDR 工具的企業理賠金額則波動較大。
- MDR 服務可加速網路攻擊事件後的復原：近一半 (47%) 使用 MDR 服務的企業可在一週內完全復原，而僅依賴端點防護的企業僅有 18% 能在一週內復原，使用 EDR/XDR 解決方案的企業則為 27%。
- MDR 服務的勒索軟體事件復原時間最為可預測，而使用 EDR/XDR 工具的企業復原時間變異較大。

資料來源：https://www.ithome.com.tw/pr/167696

MDR評估方式



DARKREADING

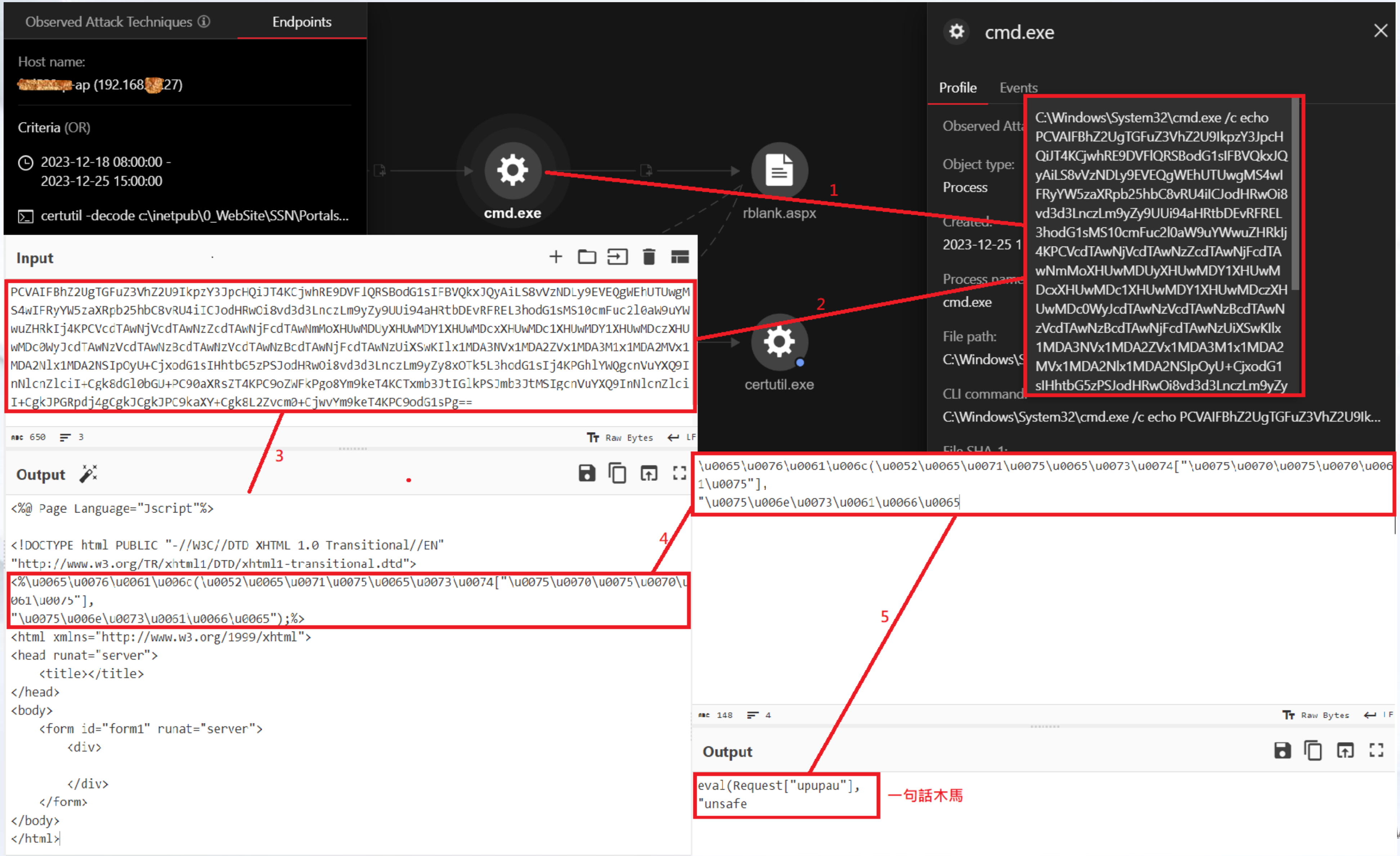
Cybersecurity Topics | World | The Edge | DR Technology

4 Key Considerations for Evaluating MDR Solutions

To assess the quality of an MDR solution, it is essential to evaluate associated EDR products and cybersecurity services separately. Consider the following factors:

1. **Malware detection and response:** An effective MDR solution should swiftly detect and respond to a wide range of threats, minimizing the dwell time of malware and preventing it from impacting the affected system.
2. **Threat detection capabilities:** The ability to detect both known and unknown threats, coupled with utilizing the latest threat intelligence, is crucial for an MDR solution's efficacy. Managed XDR solutions that offer extended capabilities should efficiently correlate security telemetry and orchestrate a comprehensive real-time response across the network.
3. **Service commitment:** Assess the MDR provider's commitment to delivering services, including around-the-clock support availability and the comprehensiveness of its service-level agreement (SLA). Additionally, consider the provider's reputation, scalability, and ability to leverage global cyber-threat intelligence.
4. **Customization and remediation:** Evaluate whether the MDR provider offers tailored products and comprehensive threat remediation and mitigation services to address your unique environment.

惡意軟體偵測和回應 (Malware detection and response)



MDR服務類型說明

功能	基礎型	一般型	進階型
通報方式	僅通報高風險事件(類SOC式通報)	高中低風險事件皆會通報	高中低風險事件皆會通報
內容撰寫	罐頭訊息居多	有較完整的事件發生原因與結果	有較完整的事件發生原因與結果
人為分析	較少的人力介入分析	較多的人力介入分析	較多的人力介入分析，進一步對事件產生的風險與影響進行分析
改善措施提供	無法提供	針對問題點提供的改善措施成效較差	可針對問題點提供有效的改善措施(較接地氣)
IR服務	無法提供	線上透過EDR進行IR	線上透過EDR進行IR+透過IR工具收取端點各種紀錄並進行IR
額外資安諮詢服務	無法提供	無法提供	可充分與客戶討論內部資安環境與改善措施

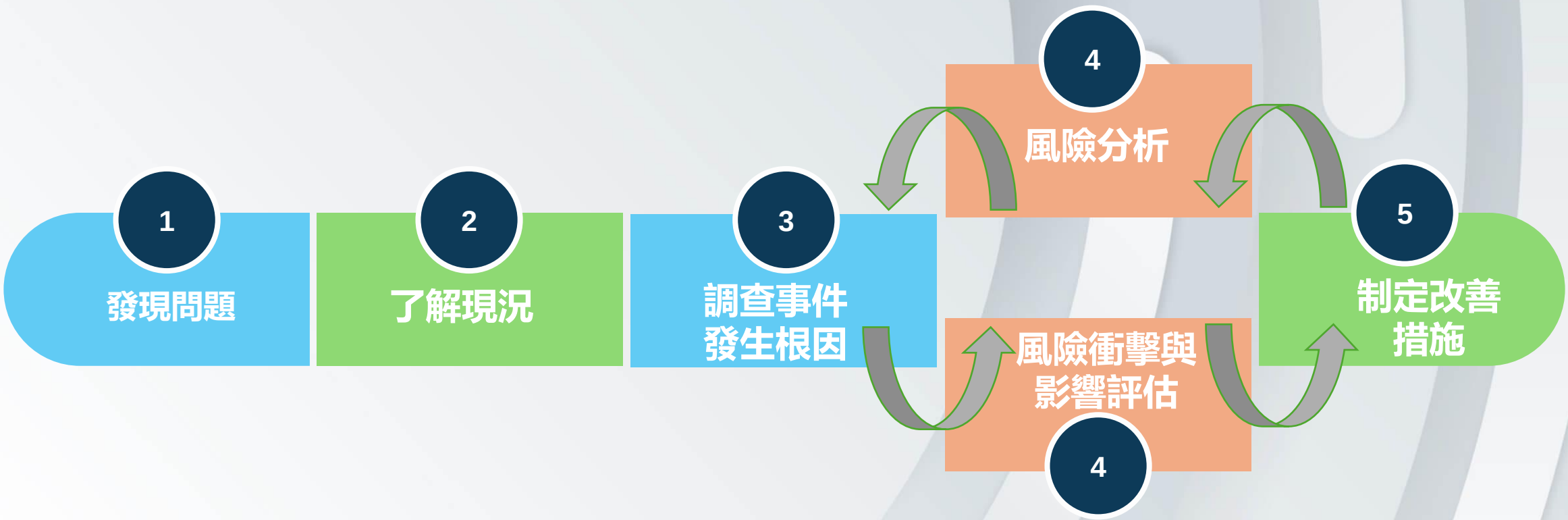
事件案例-Dump密碼

事件編號	事件名稱		
43532	Multi-stage incident involving Execution & Defense evasion on one endpoint		
開單時間	主機名稱	主機IP	風險等級
2024-12-27 09:14:20	an[redacted]xx.com		High
關聯主機			
無			
事件說明			
宏碁資訊MxDR團隊於端點"an[redacted]xx.com"上偵測到可疑檔案與活動，觸發'Multi-stage incident'相關告警。			

風險說明
駭客在主機執行這些指令，代表他們正在試圖竊取非常敏感的系統資料，並且具有極高的風險。這些指令會將 Windows 登錄檔中的關鍵區塊儲存到臨時檔案，然後駭客可以下載這些檔案並進行分析。 以下是詳細的風險說明： 1. 竊取機密資料： HKEY_LOCAL_MACHINE\SAM (安全帳戶管理員): 這個登錄檔區塊儲存了系統上的所有使用者帳戶的加密密碼雜湊值。駭客如果取得這個資料，可以嘗試破解這些雜湊值，獲取使用者帳戶的密碼，包括管理員帳戶。一旦破解成功，他們就可以完全控制系統。 HKEY_LOCAL_MACHINE\SECURITY: 這個登錄檔區塊包含了系統的安全策略設定、權限和授權資訊。駭客可以利用這些資訊來了解系統的安全架構，並尋找漏洞來提升他們的權限或繞過安全措施。 HKEY_LOCAL_MACHINE\SYSTEM: 這個登錄檔區塊包含了系統的核心配置設定、驅動程式資訊、服務設定、和啟動資訊。駭客可以利用這些資訊來了解系統的硬體和軟體環境，並可能找到漏洞來植入惡意程式碼或操縱系統行為。 2. 取得系統控制權： 透過取得上述三個登錄檔區塊的資料，駭客可以： 冒充使用者身分： 破解密碼後，他們可以登入系統，冒充合法使用者，執行惡意操作，而不容易被發現。 提升權限： 利用安全策略設定的漏洞，他們可以提升自己的權限，獲得系統的完全控制權。 植入惡意程式碼： 了解系統的啟動流程後，他們可以植入惡意程式碼，讓惡意程式在系統啟動時自動執行。 遠端控制： 透過修改系統設定，他們可以建立後門，遠端控制受感染的系統。 橫向移動： 了解系統的網路配置後，他們可以利用受感染的系統作為跳板，攻擊網路中的其他系統。 3. 後續攻擊： 這些竊取的資料通常會被駭客用於： 持久化： 建立後門，長期控制系統。 橫向移動： 攻擊網路中的其他系統。 資料外洩： 竊取敏感資料，並將其外洩到外部網路。 勒索： 加密系統資料，並勒索受害者支付贖金。

調查結果
經調查後發現，該端點’ an[redacted]xx'(10.xx.20.30)存在可疑檔案： "C:\Windows\Temp\OOqISkRwVWUeFp_w6.exe" SHA256:231434379a0962e78fa818c85874ad5a31afc93ec8a038c033cc27c09b0c17e9 "C:\Windows\Temp\OOqISkRwVWUeFp_w6.txt" SHA256:30181df62ea363ce2d1647f17ad5e50679721ca0dc4bb1e068b9b04995dfcab9 後續並偵測到可疑的PowerShell指令與其他疑似竊取資料的活動，如： "reg.exe" save HKEY_LOCAL_MACHINE\sam\ C:\Windows\Temp\OOqISkRwVWUeFp_sa.png /y "reg.exe" save HKEY_LOCAL_MACHINE\security\ C:\Windows\Temp\OOqISkRwVWUeFp_se.png /y "reg.exe" save HKEY_LOCAL_MACHINE\system\ C:\Windows\Temp\OOqISkRwVWUeFp_sy.png /y 上述指令將會將機碼資料存至'C:\Windows\Temp\'資料夾下，並透過圖片檔案名稱來規避偵測。
立即處理建議
建議將此台端點暫先離線，清空上述暫存檔路徑： ‘C:\Windows\Temp\’ ，並進行端點全機掃描找出是否仍有其他潛在的可疑程式，弱有需要請啟動IR服務。
後續改善建議
無
發現惡意程式或連線之惡意中繼站
未發現惡意程式或連線至惡意中繼站行為。

即時威脅監控服務架構-問題處理原則



事件案例-透過w3wp.exe執行command

事件編號	事件名稱		
WB-16047-20231225-00000	File Deobfuscation via CertUtil		
開單時間	主機名稱	主機IP	風險等級
2023-12-25 15:50:56	[redacted]ap	192.168.[redacted].27	Hgh
關聯主機			
無			
事件說明			
宏碁資訊MxDR團隊發現主機名稱[redacted]ap觸發"System Network Information Discovery via IIS"、"Potential Information Gathering"、"System Information Discovery via IIS Webshell Command"、"File Deobfuscation via CertUtil"事件。			
調查結果			
此事件共出現透過CertUtil將c:\inetpub\0_WebSite\SSN\Portals_default\rblank.aspx解譯為c:\inetpub\0_WebSite\SSN\Portals_default\sblank.aspx、透過w3wp.exe執行cmd.exe，並執行whoami與ipconfig蒐集資訊等可疑行為，經確認為駭客成功上傳webshell所導致之一連串攻擊。			
立即處理建議			
請對該主機進行重灌作業。			

事件案例-事件調查(IR)

- 12/25 15:47~15:48 發現有rblank.aspx與sblank.aspx被compiled的狀況 。

Filename #1	Std Info Creation d	Std Info Modificati	Std Info Access dat	Std Info Entry date	FN Info Creatior
/Windows/Temp/RazorEngine_rsd4yqxo.2yc/xqp4xvuh.0.cs	2023/12/25 15:51	2023/12/25 15:51	2023/12/25 15:51	2023/12/25 15:51	2023/12/25 15:
/Windows/Temp/RazorEngine_rsd4yqxo.2yc/xqp4xvuh.cmdline	2023/12/25 15:51	2023/12/25 15:51	2023/12/25 15:51	2023/12/25 15:51	2023/12/25 15:
/Windows/Temp/RazorEngine_kzbf4rdl.ihn/CompiledRazorTemplates.Dynamic.RazorEngine_46c6277d2c4c49f99bfa72e677dadc30x10.dll	2023/12/25 15:51	2023/12/25 15:51	2023/12/25 15:51	2023/12/25 15:51	2023/12/25 15:
/Windows/Temp/RazorEngine_kzbf4rdl.ihn/kbtemd3m.out	2023/12/25 15:51	2023/12/25 15:51	2023/12/25 15:51	2023/12/25 15:51	2023/12/25 15:
/Windows/Temp/RazorEngine_kzbf4rdl.ihn/kbtemd3m.err	2023/12/25 15:51	2023/12/25 15:51	2023/12/25 15:51	2023/12/25 15:51	2023/12/25 15:
/Windows/Temp/RazorEngine_kzbf4rdl.ihn	2023/12/25 15:51	2023/12/25 15:51	2023/12/25 15:51	2023/12/25 15:51	2023/12/25 15:
/Windows/Temp/RazorEngine_kzbf4rdl.ihn/kbtemd3m.tmp	2023/12/25 15:51	2023/12/25 15:51	2023/12/25 15:51	2023/12/25 15:51	2023/12/25 15:
/Windows/Temp/RazorEngine_kzbf4rdl.ihn/kbtemd3m.0.cs	2023/12/25 15:51	2023/12/25 15:51	2023/12/25 15:51	2023/12/25 15:51	2023/12/25 15:
/Windows/Temp/RazorEngine_kzbf4rdl.ihn/kbtemd3m.cmdline	2023/12/25 15:51	2023/12/25 15:51	2023/12/25 15:51	2023/12/25 15:51	2023/12/25 15:
Windows/Microsoft.NET/Framew0xf00x01rk64/v4.0.30319/Temporary ASP.NET Files/root/0a541698/8aa83b32/App_Web_h1ntjdcf.dll	2023/12/25 15:50	2023/12/25 15:50	2023/12/25 15:50	2023/12/25 15:50	2023/12/25 15:
Windows/Microsoft.NET/Framew0xf00x01rk64/v4.0.30319/Temporary ASP.NET Files/root/0a541698/8aa83b32/sblank.aspx.ba6a84b8.compiled	2023/12/25 15:48	2023/12/25 15:50	2023/12/25 15:50	2023/12/25 15:50	2023/12/25 15:
Windows/Microsoft.NET/Framew0xf00x01rk64/v4.0.30319/Temporary ASP.NET Files/root/0a541698/8aa83b32/subhost.aspx.ba6a84b8.compiled	2023/12/25 15:47	2023/12/25 15:47	2023/12/25 15:47	2023/12/25 15:47	2023/12/25 15:
Windows/Microsoft.NET/Framew0xf00x01rk64/v4.0.30319/Temporary ASP.NET Files/root/0a541698/8aa83b32/App_Web_ce0aey1j.dll	2023/12/25 15:47	2023/12/25 15:47	2023/12/25 15:47	2023/12/25 15:47	2023/12/25 15:
Windows/Microsoft.NET/Framew0xf00x01rk64/v4.0.30319/Temporary ASP.NET Files/root/0a541698/8aa83b32/rblank.aspx.ba6a84b8.compiled	2023/12/25 15:47	2023/12/25 15:47	2023/12/25 15:47	2023/12/25 15:47	2023/12/25 15:
/Windows/Temp/RazorEngine_d2ncmlw2.tfa/CompiledRazorTemplates.Dynamic.RazorEngine_90afd82dad744352866f21c3f08835e0x0d.dll	2023/12/25 15:31	2023/12/25 15:31	2023/12/25 15:31	2023/12/25 15:31	2023/12/25 15:
NoFNRecord	2023/12/25 15:31	2023/12/25 15:31	2023/12/25 15:31	2023/12/25 15:31	NoFNRecord
/Windows/Temp/RazorEngine_d2ncmlw2.tfa/ga2bruuc.out	2023/12/25 15:31	2023/12/25 15:31	2023/12/25 15:31	2023/12/25 15:31	2023/12/25 15:
/Windows/Temp/RazorEngine_d2ncmlw2.tfa/ga2bruuc.err	2023/12/25 15:31	2023/12/25 15:31	2023/12/25 15:31	2023/12/25 15:31	2023/12/25 15:
/Windows/Temp/RazorEngine_d2ncmlw2.tfa	2023/12/25 15:31	2023/12/25 15:31	2023/12/25 15:31	2023/12/25 15:31	2023/12/25 15:
/Windows/Temp/RazorEngine_d2ncmlw2.tfa/ga2bruuc.tmp	2023/12/25 15:31	2023/12/25 15:31	2023/12/25 15:31	2023/12/25 15:31	2023/12/25 15:
/Windows/Temp/RazorEngine_d2ncmlw2.tfa/ga2bruuc.0.cs	2023/12/25 15:31	2023/12/25 15:31	2023/12/25 15:31	2023/12/25 15:31	2023/12/25 15:
/Windows/Temp/RazorEngine_d2ncmlw2.tfa/ga2bruuc.cmdline	2023/12/25 15:31	2023/12/25 15:31	2023/12/25 15:31	2023/12/25 15:31	2023/12/25 15:

事件案例-事件調查(IR)

- 進一步調查，該時間有IP 61.62.215.70對該網站連線，另外往前追溯，發現IP 125.228.28.143有探查漏洞行為。

```
2023-12-25 07:25:31 192.168.27.63 GET /Resources/libraries/jQuery-UI/01_11_03/jquery-ui.js cdv=799 443 - 125.228.28.143 Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+10_15_7)+AppleWebKit/53
2023-12-25 07:25:31 192.168.27.63 GET /images/Flags/vi-VN.gif - 443 - 125.228.28.143 Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+10_15_7)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/120
2023-12-25 07:25:31 192.168.27.63 GET /Resources/Shared/scripts/initWidgets.js - 443 - 125.228.28.143 Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+10_15_7)+AppleWebKit/537.36+(KHTML,+like+
2023-12-25 07:25:31 192.168.27.63 GET /Portals/_default/Skins/Gravity/images/globe.png - 443 - 125.228.28.143 Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+10_15_7)+AppleWebKit/537.36+(KHTM
2023-12-25 07:25:32 192.168.27.63 GET /Resources/Shared/scripts/initWidgets.js - 443 - 125.228.28.143 Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+10_15_7)+AppleWebKit/537.36+(KHTML,+like+
2023-12-25 07:25:32 192.168.27.63 GET /Resources/Shared/scripts/DotNetNukeAjaxShared.js _=1703489088614 443 - 125.228.28.143 Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+10_15_7)+AppleWebK
2023-12-25 07:25:32 192.168.27.63 GET /favicon.ico - 443 - 125.228.28.143 Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+10_15_7)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/120.0.0.0+Safa
2023-12-25 07:25:33 192.168.27.63 GET /Resources/Shared/scripts/widgets.js _=1703489088615 443 - 125.228.28.143 Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+10_15_7)+AppleWebKit/537.36+(KH
2023-12-25 07:26:24 192.168.27.63 GET /_ - 443 - 125.228.28.143 Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+10_15_7)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/120.0.0.0+Safari/537.36
2023-12-25 07:27:32 192.168.27.63 GET /_ - 443 - 125.228.28.143 Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+10_15_7)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/120.0.0.0+Safari/537.36
2023-12-25 07:27:52 192.168.27.63 GET /_ - 443 - 125.228.28.143 Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+10_15_7)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/120.0.0.0+Safari/537.36
2023-12-25 07:28:56 192.168.27.63 GET /_ - 443 - 125.228.28.143 Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+10_15_7)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/120.0.0.0+Safari/537.36
2023-12-25 07:29:01 192.168.27.63 GET /_ - 443 - 125.228.28.143 Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+10_15_7)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/120.0.0.0+Safari/537.36
2023-12-25 07:29:49 192.168.27.63 GET /_ - 443 - 125.228.28.143 Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+10_15_7)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/120.0.0.0+Safari/537.36
2023-12-25 07:29:55 192.168.27.63 GET /_ - 443 - 125.228.28.143 Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+10_15_7)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/120.0.0.0+Safari/537.36
2023-12-25 07:30:44 192.168.27.63 GET /_ - 443 - 125.228.28.143 Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+10_15_7)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/120.0.0.0+Safari/537.36
2023-12-25 07:30:50 192.168.27.63 GET /_ - 443 - 125.228.28.143 Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+10_15_7)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/120.0.0.0+Safari/537.36
2023-12-25 07:31:26 192.168.27.63 GET /_ - 443 - 125.228.28.143 Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+10_15_7)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/120.0.0.0+Safari/537.36
2023-12-25 07:31:33 192.168.27.63 GET /_ - 443 - 125.228.28.143 Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+10_15_7)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/120.0.0.0+Safari/537.36
2023-12-25 07:32:46 192.168.27.63 GET /_ - 443 - 125.228.28.143 Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+10_15_7)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/120.0.0.0+Safari/537.36
2023-12-25 07:32:50 192.168.27.63 GET /_ - 443 - 125.228.28.143 Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+10_15_7)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/120.0.0.0+Safari/537.36
2023-12-25 07:33:40 192.168.27.63 GET /_ - 443 - 125.228.28.143 Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+10_15_7)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/120.0.0.0+Safari/537.36
2023-12-25 07:41:51 192.168.27.63 GET /_ - 443 - 61.62.215.70 Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+10_15_7)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/120.0.0.0+Safari/537.36 -
2023-12-25 07:41:56 192.168.27.63 GET /_ - 443 - 61.62.215.70 Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+10_15_7)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/120.0.0.0+Safari/537.36 -
2023-12-25 07:43:01 192.168.27.63 GET /_ - 443 - 61.62.215.70 Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+10_15_7)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/120.0.0.0+Safari/537.36 -
2023-12-25 07:43:14 192.168.27.63 GET /_ - 443 - 61.62.215.70 Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+10_15_7)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/120.0.0.0+Safari/537.36 -
2023-12-25 07:46:57 192.168.27.63 GET /_ - 443 - 61.62.215.70 Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+10_15_7)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/120.0.0.0+Safari/537.36 -
2023-12-25 07:47:26 192.168.27.63 GET /Portals/_default/rblank.aspx - 443 - 61.62.215.70 Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+10_15_7)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome
2023-12-25 07:48:27 192.168.27.63 GET /_ - 443 - 61.62.215.70 Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+10_15_7)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/120.0.0.0+Safari/537.36 -
2023-12-25 07:48:38 192.168.27.63 GET /Portals/_default/sblank.aspx - 443 - 61.62.215.70 Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+10_15_7)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome
2023-12-25 07:49:04 192.168.27.63 POST /Portals/_default/sblank.aspx - 443 - 61.62.215.70 Mozilla/5.0+(Windows+NT+5.1)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/34.0.1866.237+Saf
2023-12-25 07:49:15 192.168.27.63 POST /Portals/_default/sblank.aspx - 443 - 61.62.215.70 Mozilla/5.0+(compatible;+MSIE+9.0;+Windows+NT+6.1;+WOW64;+Trident/5.0;+.NET+CLR+3.5.30729;+.
2023-12-25 07:49:18 192.168.27.63 POST /Portals/_default/sblank.aspx - 443 - 61.62.215.70 Mozilla/5.0+(Windows;+U;+Windows+NT+6.1;+fr-FR)+AppleWebKit/533.20.25+(KHTML,+like+Gecko)+Ve
2023-12-25 07:49:29 192.168.27.63 POST /Portals/_default/sblank.aspx - 443 - 61.62.215.70 Mozilla/5.0+(Windows+NT+6.2;+rv:22.0)+Gecko/20130405+Firefox/23.0 - 200 0 0 26
2023-12-25 07:49:32 192.168.27.63 POST /Portals/_default/sblank.aspx - 443 - 61.62.215.70 Mozilla/5.0+(Windows+NT+6.2;+Win64;+x64;+rv:27.0)+Gecko/20121011+Firefox/27.0 - 200 0 0 29
2023-12-25 07:49:38 192.168.27.63 POST /Portals/_default/sblank.aspx - 443 - 61.62.215.70 Opera/9.80+(X11;+Linux+x86_64;+U;+bg)+Presto/2.8.131+Version/11.10 - 200 0 0 25
2023-12-25 07:50:25 192.168.27.63 POST /Portals/_default/sblank.aspx - 443 - 61.62.215.70 Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+10.6;+rv:25.0)+Gecko/20100101+Firefox/25.0 - 200 0 0
2023-12-25 07:50:28 192.168.27.63 POST /Portals/_default/sblank.aspx - 443 - 61.62.215.70 Opera/9.80+(X11;+Linux+i686;+U;+es-ES)+Presto/2.8.131+Version/11.11 - 200 0 0 258
2023-12-25 07:50:42 192.168.27.63 POST /Portals/_default/sblank.aspx - 443 - 61.62.215.70 Mozilla/5.0+(compatible;+MSIE+9.0;+Windows+NT+6.1;+WOW64;+Trident/5.0;+.NET+CLR+3.5.30729;+.
2023-12-25 07:51:11 192.168.27.63 POST /Portals/_default/sblank.aspx - 443 - 61.62.215.70 Opera/9.80+(X11;+Linux+i686;+U;+hu)+Presto/2.9.168+Version/11.50 - 200 0 0 24
2023-12-25 07:51:17 192.168.27.63 POST /Portals/_default/sblank.aspx - 443 - 61.62.215.70 Opera/9.80+(Windows+NT+6.1;+WOW64;+U;+pt)+Presto/2.10.229+Version/11.62 - 200 0 0 19
2023-12-25 07:53:42 192.168.27.63 POST /Portals/_default/sblank.aspx - 443 - 61.62.215.70 Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+10_7_3)+AppleWebKit/534.55.3+(KHTML,+like+Gecko)+Vers
2023-12-25 07:53:49 192.168.27.63 POST /Portals/_default/sblank.aspx - 443 - 61.62.215.70 Mozilla/5.0+(Windows+NT+6.2;+Win64;+x64;+rv:27.0)+Gecko/20121011+Firefox/27.0 - 200 0 0 310
```

事件案例-事件調查(IR)

- 分析入侵過程發現IP 61.62.215.70 有連續存取”/_”路徑，導致Server回覆404代碼，故推測駭客利用CVE-2017-9822 漏洞進行檔案上傳與執行任意代碼攻擊。
- 漏洞詳細說明請參考:
- https://blog.csdn.net/xuexi056/article/details/133107101
- https://paper.seebug.org/365/。

```
12-25 07:29:49 192.168.27.63 GET /_ - 443 - 125.228.28.143 Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+10_15_7)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/120.0.0.0+Safari/537.36 - 404
12-25 07:29:55 192.168.27.63 GET /_ - 443 - 125.228.28.143 Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+10_15_7)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/120.0.0.0+Safari/537.36 - 404
12-25 07:30:44 192.168.27.63 GET /_ - 443 - 125.228.28.143 Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+10_15_7)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/120.0.0.0+Safari/537.36 - 404
12-25 07:30:50 192.168.27.63 GET /_ - 443 - 125.228.28.143 Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+10_15_7)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/120.0.0.0+Safari/537.36 - 404
12-25 07:31:26 192.168.27.63 GET /_ - 443 - 125.228.28.143 Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+10_15_7)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/120.0.0.0+Safari/537.36 - 404
12-25 07:31:33 192.168.27.63 GET /_ - 443 - 125.228.28.143 Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+10_15_7)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/120.0.0.0+Safari/537.36 - 404
12-25 07:32:46 192.168.27.63 GET /_ - 443 - 125.228.28.143 Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+10_15_7)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/120.0.0.0+Safari/537.36 - 404
12-25 07:32:50 192.168.27.63 GET /_ - 443 - 125.228.28.143 Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+10_15_7)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/120.0.0.0+Safari/537.36 - 404
12-25 07:33:40 192.168.27.63 GET /_ - 443 - 125.228.28.143 Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+10_15_7)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/120.0.0.0+Safari/537.36 - 404
12-25 07:41:51 192.168.27.63 GET /_ - 443 - 61.62.215.70 Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+10_15_7)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/120.0.0.0+Safari/537.36 - 404 0
12-25 07:41:56 192.168.27.63 GET /_ - 443 - 61.62.215.70 Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+10_15_7)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/120.0.0.0+Safari/537.36 - 404 0
12-25 07:43:01 192.168.27.63 GET /_ - 443 - 61.62.215.70 Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+10_15_7)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/120.0.0.0+Safari/537.36 - 404 0
12-25 07:43:14 192.168.27.63 GET /_ - 443 - 61.62.215.70 Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+10_15_7)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/120.0.0.0+Safari/537.36 - 404 0
12-25 07:46:57 192.168.27.63 GET /_ - 443 - 61.62.215.70 Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+10_15_7)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/120.0.0.0+Safari/537.36 - 404 0
12-25 07:47:26 192.168.27.63 GET /Portals/_default/rblank.aspx - 443 - 61.62.215.70 Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+10_15_7)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/120.
12-25 07:48:27 192.168.27.63 GET /_ - 443 - 61.62.215.70 Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+10_15_7)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/120.0.0.0+Safari/537.36 - 404 0
12-25 07:48:38 192.168.27.63 GET /Portals/_default/sblank.aspx - 443 - 61.62.215.70 Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+10_15_7)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/120.
12-25 07:49:04 192.168.27.63 POST /Portals/_default/sblank.aspx - 443 - 61.62.215.70 Mozilla/5.0+(Windows+NT+5.1)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/34.0.1866.237+Safari/5
12-25 07:49:15 192.168.27.63 POST /Portals/_default/sblank.aspx - 443 - 61.62.215.70 Mozilla/5.0+(compatible;+MSIE+9.0;+Windows+NT+6.1;+WOW64;+Trident/5.0;+.NET+CLR+3.5.30729;+.NET+C
12-25 07:49:18 192.168.27.63 POST /Portals/_default/sblank.aspx - 443 - 61.62.215.70 Mozilla/5.0+(Windows;+U;+Windows+NT+6.1;+fr-FR)+AppleWebKit/533.20.25+(KHTML,+like+Gecko)+Version
12-25 07:49:29 192.168.27.63 POST /Portals/_default/sblank.aspx - 443 - 61.62.215.70 Mozilla/5.0+(Windows+NT+6.2;+rv:22.0)+Gecko/20130405+Firefox/23.0 - 200 0 0 26
12-25 07:49:32 192.168.27.63 POST /Portals/_default/sblank.aspx - 443 - 61.62.215.70 Mozilla/5.0+(Windows+NT+6.2;+Win64;+x64;+rv:27.0)+Gecko/20121011+Firefox/27.0 - 200 0 0 29
12-25 07:49:38 192.168.27.63 POST /Portals/_default/sblank.aspx - 443 - 61.62.215.70 Opera/9.80+(X11;+Linux+x86_64;+U;+bg)+Presto/2.8.131+Version/11.10 - 200 0 0 25
12-25 07:50:25 192.168.27.63 POST /Portals/_default/sblank.aspx - 443 - 61.62.215.70 Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+10.6;+rv:25.0)+Gecko/20100101+Firefox/25.0 - 200 0 0 34
```

調查結果-透過w3wp.exe執行command

事件編號	事件名稱		
WB-16047-20231225-00000	File Deobfuscation via CertUtil		
開單時間	主機名稱	主機IP	風險等級
2023-12-25 15:50:56	[redacted]-ap	192.168[redacted].27	Hgh
關聯主機			
無			
事件說明			
宏碁資訊MxDR團隊發現主機名稱[redacted]-ap觸發"System Network Information Discovery via IIS"、"Potential Information Gathering"、"System Information Discovery via IIS Webshell Command"、"File Deobfuscation via CertUtil"事件。			
調查結果			
此事件共出現透過CertUtil將c:\inetpub\0_WebSite\SSN\Portals_default\rblank.aspx解譯為c:\inetpub\0_WebSite\SSN\Portals_default\sblank.aspx、透過w3wp.exe執行cmd.exe，並執行whoami與ipconfig蒐集資訊等可疑行為，經確認為駭客成功上傳webshell所導致之一連串攻擊。			
立即處理建議			
請對該主機進行重灌作業。			
駭客使用此混淆方式目的是要繞過防毒軟體偵測。 再駭客上傳webshell後，陸續發現駭客有對該主機執行whoami、ipconfig等行為，但尚未發現駭客有更進一步的其他攻擊行為，故研判傷害沒有擴大跡象。			
立即處理建議			
1.盡快移除以下兩個檔案 c:\inetpub\0_WebSite\SSN\Portals_default\rblank.aspx c:\inetpub\0_WebSite\SSN\Portals_default\sblank.aspx 2.建議關閉該網站接收處理cookie之功能 3.建議將DNN升級至最新版本			

風險說明
駭客成功上傳 Webshell，意味著他們已經在你的網站伺服器上取得了一個極度危險的後門。這會導致一系列嚴重的安全風險，可能對你的業務造成毀滅性的影響。 以下是具體風險的詳細說明： 1. 完全控制網站伺服器: 遠端執行任意命令: Webshell 本質上是一個允許駭客透過 Web 瀏覽器執行伺服器命令列指令的介面。這意味著駭客可以執行任何操作，就像他們直接在伺服器上操作一樣。 讀取、修改、刪除檔案: 他們可以隨意讀取伺服器上的任何檔案，包括程式碼、設定檔、資料庫連接字串等敏感資訊。 他們也可以修改或刪除檔案，破壞網站功能，甚至癱瘓整個網站。 上傳和下載檔案: 駭客可以利用 Webshell 上傳惡意程式碼到伺服器，或者下載伺服器上的敏感資料。 2. 資料外洩: 竊取使用者資料: 駭客可以利用 Webshell 存取網站的資料庫，竊取使用者帳戶、密碼、信用卡資訊等敏感資料。 竊取商業機密: 如果你的網站儲存了商業機密、客戶資料、產品設計等重要資訊，駭客也可以利用 Webshell 將其竊取。 3. 伺服器被當作跳板: 發動 DDoS 攻擊: 駭客可以利用你的伺服器作為殭屍網路的一部分，發動分散式阻斷服務 (DDoS) 攻擊，癱瘓其他網站或網路服務。 攻擊其他系統: 他們可以利用你的伺服器作為跳板，攻擊你內部網路中的其他系統，擴大攻擊範圍。 散播惡意程式: 你的伺服器可能被用來散播惡意程式碼，感染其他使用者的電腦。 4. 網站被竄改: 惡意程式碼注入: 駭客可以在你的網站中注入惡意程式碼，例如惡意廣告、釣魚連結等，將使用者重新導向到惡意網站，竊取他們的資訊。 網頁內容篡改: 他們可以竄改網站的內容，發布不實資訊、政治宣傳等，損害你的聲譽。 植入挖礦程式: 駭客可以在你的網站上植入加密貨幣挖礦程式，利用訪客的電腦資源進行挖礦，增加伺服器負載，影響網站效能。 5. 伺服器被勒索: 加密檔案勒索: 駭客可以利用 Webshell 加密伺服器上的所有檔案，然後勒索你支付贖金才能解密。 6. 聲譽受損與法律責任: 客戶信任度降低: 如果你的網站發生資料外洩事件，客戶的信任度會大幅降低，影響你的業務。 法律訴訟與罰款: 你可能需要承擔法律責任，並支付巨額罰款，例如違反 GDPR 等資料保護法規。

事件調查(IR)的差異

類型	線上透過EDR進行IR	透過IR工具收取端點各種紀錄並進行IR
花費人力時間	較短 (主要針對EDR通報事件進型分析，可能有少部分的Threat Hunting)	較長 (需耗費大量人力分析蒐集之資料)
技術要求	較低 (以EDR提供之功能為主)	較高 (須熟悉各種IR工具、駭客思維與IR方法論)
事件還原詳細度	較低(以EDR通報事件為主體)	較高(除了EDR通報事件，亦會蒐集其他log進行分析，ex. Event log, MFT, Amcache, ShimCache, Registry, Web log, ….)
可否找到駭客利用之所有工具與惡意程式	較不完整(以EDR通報事件為主體)	較完整(除了利用EDR通報事件查找惡意程式，亦會利用駭客邏輯思維搜捕其他惡意程式與駭客利用之工具)
可否調查利用Web漏洞之入侵根因	相當困難(EDR無法紀錄Web log)	可 (有蒐集Web log，故可分析出駭客利用何種Web漏洞入侵)
給予之改善建議完善度	較低(較難調查出事件發生根因，故較難提供針對根因之改善方式)	較高(可查出事件發生根因，故可提供針對根因之改善方式)
可否避免重複發生相同事件	較難(由於難以找到事件發生根因，難以針對事件根因進行改善，使駭客可重複利用該漏洞進行入侵)	可 (可查出事件發生根因，並針對根因進行改善，使駭客無法再利用該漏洞進行入侵)


The Best
is Yet to Come !
AEB 宏碁資訊
最懂地端的雲端公司 企業生成式AI加速器

2025資安大會-AEB 議程問卷： 重灌人生太淒涼，來點不一樣的 MDR

MDR服務類型說明

基礎型

- 僅通報高風險事件(類SOC式通報)
- 罐頭訊息居多
- 較少的人力介入分析

一般型

- 高中低風險事件皆會通報
- 有較完整的事件發生原因與結果
- 較多的人力介入分析
- 針對問題點提供的改善措施成效較差
- 線上透過EDR進行IR

進階型

- 高中低風險事件皆會通報
- 有較完整的事件發生原因與結果
- 較多的人力介入分析，進一步對事件產生的風險與影響進行分析
- 可針對問題點提供有效的改善措施(較接地氣)
- 線上透過EDR進行IR+透過IR工具收取端點各種紀錄並進行IR
- 可充分與客戶討論內部資安環境與改善措施