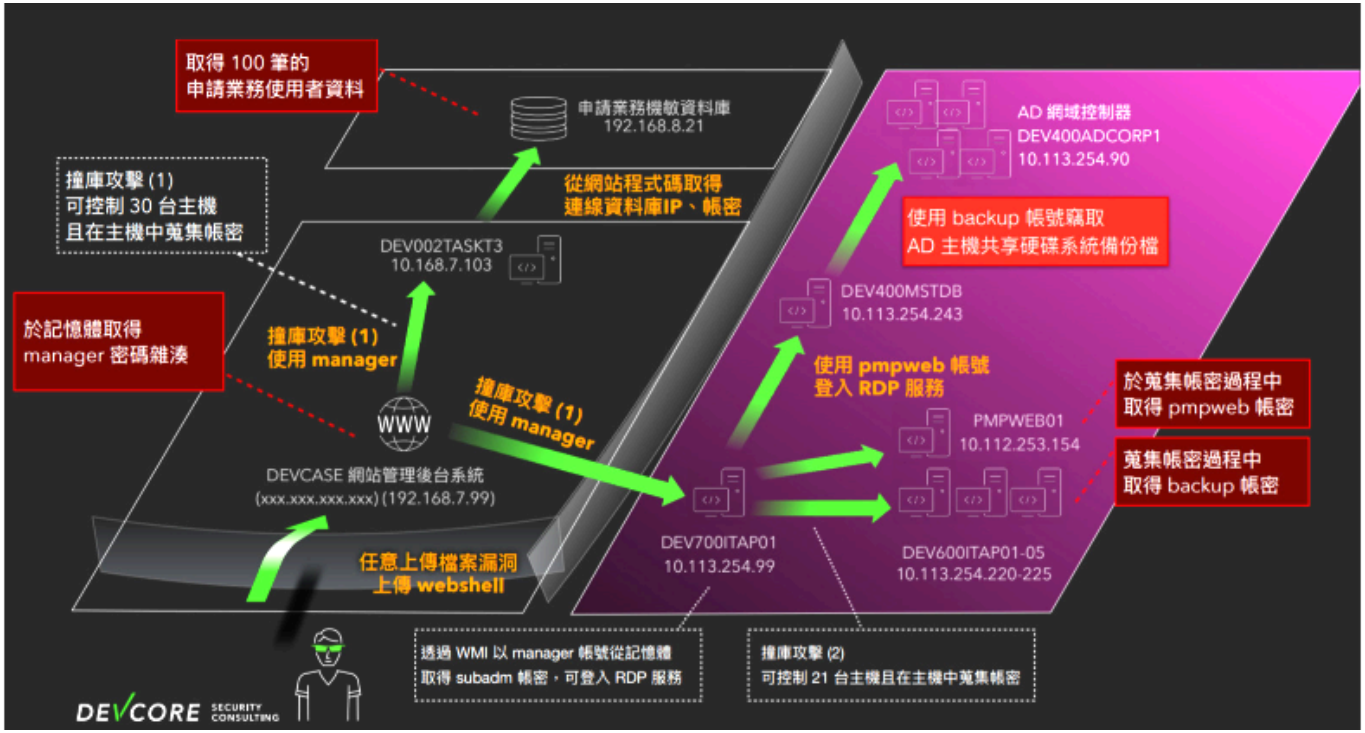
【用Cyber Defense Matrix搭配資安框架改善資安弱點】資安策略成效要靠真實威脅調整

資安防禦層面廣而無從下手，戴夫寇爾事業發展經理鍾澤華表示，可借助CDM進行規畫，盤點需強化的程序、控制措施與設備

文/ 羅正漢 | 2020-09-24 發表



【以紅隊演練結果為例，找出防禦不足的環節】資安策略的基礎是資安框架，但其有效性需靠真實威脅調整，為了說明這樣的概念，戴夫寇爾執行長翁浩正以一場紅隊演練為例，當中有網站管理後臺系統具任意上傳檔案漏洞，偵測機制不足與內網被突破，還有帳號密碼問題，因此，制定改善方針就是關鍵，才能幫助資安策略上的微調。圖片來源 / 戴夫寇爾

企業在擬定資安策略後，如何驗證，以及要讓資安框架更有效果，仍要靠真實威脅調整。戴夫寇爾執行長兼共同創辦人翁浩正表示，他們從自身幫助客戶進行紅隊演練的經驗，來說明在面對真實威脅時，可以如何透過活用資安框架，去緩解一連串的脆弱環節。

在先前的部分，他們已經說明了各管理階層的考量，包含：資安長、資安官（資安高階主管）、資安主管，與第一線資安人員，由上而下分別對應風險、程序、控制與技術的層面，各自有可以參考的資安框架，視為資安策略的基礎。但不僅於此，從攻擊角度來看，這樣的4層架構，其實也能有助於做好資安的驗證與精進。

戴夫寇爾事業發展經理鍾澤華表示，當發生資安事件或進行攻防演練，也可透過由下而上的方式，來檢視每一層是否能做好管控。

以最下一層的資安設備及服務而言，他舉例，當廠商聲稱有一個100%防禦無敵的解決方案，企業該如何搞懂實際該解決方案的適用範疇？對此，他談到了一個安全模型Cyber Defense Matrix（CDM）。

這是2016年美國銀行擔任首席安全科學家的Sounil Yu所提出，並納入OWASP，或稱之為OWASP CDM，目前臺灣較少人提及。

簡單來說，這個CDM其實就是一個5乘5的矩陣，橫軸分別是NIST CSF的五大類別，項目包括：識別、保護、偵測、回應、復原，並且加入了以資產類別畫分的縱軸，項目分別是：設備（Devices）、應用程式（Application）、網路（Network），資料（Data）與人員（User）。

透過這樣的CDM矩陣，企業要知道每個解決方案所涵蓋的面向，就能有較容易的方式，去看待與盤點這些產品。換言之，用CDM矩陣將能有更直觀的方式，掌握到企業本身的資安缺口。而且，這種衡量方式，可以更簡單去理解，一個解決方案無法解決一切問題。

不過，翁浩正也強調，這並不是要企業拼命買設備與解決方案，以填補資安缺口。若將先前所提的4層架構立體化，這個CDM矩陣，不只是可以應用在最下方的技術層，他們也提出可將不同層串接在一起的概念，如此一來，企業將可知道攻擊由下而上穿透時，有那些部分還沒有顧到。他舉例，企業除了從最下層的方案面來著手，往上也能藉由流程面的資安框架來因應，補足設備面的不足，但也不能全靠流程面來解決就是，因此需要平衡。

對於資安策略規畫與精進，可從真實威脅來驗證

為了讓大家更好理解上述概念，翁浩正與鍾澤華也特別從他們紅隊演練的經驗，透過實際的案例來說明。企業除了由上而下做到資安策略規畫，也能利用上述資安框架與模型，透過演練結果由下而上去回顧與精進。

利用紅隊演練結果案例找出實際威脅

翁浩正以一場實際紅隊演練來說明。他指出，在攻擊過程中，他們先是找出了該企業對外網站上的漏洞，這是企業率先遭攻擊的防禦弱點。

值得注意的是，該網站是一個網站管理後臺系統，但因疏於管理，所以被他們找到了任意上傳檔案漏洞，因此可以上傳Webshell後門，之後透過記憶體分析得到管理者密碼的雜湊，經破解密碼，進而取得一個管理者的關鍵帳號，而這個帳號能夠登入另外30多臺主機，他們在這些主機上蒐集帳密後，又找到一個主機的網站程式碼，因此取得關鍵連線資料庫的IP位址與帳號密碼，取得了企業的申請業務的敏感個資資料。

接下來，紅隊進一步瞄準目標內網的控制權，由於他們先前入侵的網站管理後臺系統，本身也有串連到內部網路，因此紅隊循此路徑，就進入了企業的內部網路。他們先是透過WMI取得內網一臺主機的管理者帳

號，仿效先前的攻擊手法，從記憶體分析出更多的帳號與密碼，包括取得了可登入RDP服務的子管理者帳密，可控制21臺主機並且持續蒐集帳密。

特別的是，他們還得到了另一臺主機的PMPweb帳號密碼，以及從這些主機中得到一個備份的帳號密碼，最終，他們藉由取得的一個網域 / 目錄（AD）伺服器的備份檔，找出AD內的密碼雜湊，破解後進而得到大量使用者的資料。翁浩正提醒，現在許多的備份方案，都希望企業的備份帳號具有最高權限，等同於管理者帳號，由於這個備份帳號可以取得全部的資料，一旦被竊取，後果相當嚴重。

從上述攻擊結果來看，企業會發現防禦有那些問題？從一般簡單的推想來看，鍾澤華說明，首先就是程式寫不好，所以該網站管理後臺系統可以被上傳Webshell，還有就是在偵測機制上的不足，回應時間不夠即時，以及帳號密碼或網路管理的問題，但是，問題就只有這樣嗎？

對此，鍾澤華特別強調，這也是企業為何需要框架或標準的原因，因為這些內容其實已經設想了多數常犯的錯誤，而透過將資安標準結合前述CDM矩陣的使用方式，將讓企業可以更精確的盤點出完整防護能力，例如，在防禦縱深的哪一階段沒有做好，才能知道要挑選何種設備、增加什麼樣的程序，以及需要強化的控制措施。

如果沒有這樣的架構，鍾澤華強調，企業將無法知道問題，也就是看出風險或安全問題的全貌，而且，只要這些問題有一小部分沒有解決，這意謂著這個風險其實是持續存在的。

該如何依據攻擊演練結果修正資安問題？

對於企業待補強的防禦縱深機制，鍾澤華表示，在使用方法上，CDM矩陣不只適用於技術層，具體而言，往上也能對應到控制層與程序層，透過資安框架的活用，並要能夠瞭解不同層之間如何串接在一起。

在控制層依循CIS CSC來管控

他以控制層為例，透過資安框架CIS CSC控制項搭配CDM矩陣，說明上述紅隊演練結果所對應的內容。

在上述紅隊演練結果中，可以先整理出可對應的相關CSC控制項，總共包含21項，例如：4.2的變更預設密碼，6.3的開啟更詳盡的日誌記錄，12.1的維護網路邊界清單等。

而這些項目，將可對應到CDM矩陣中的不同位置，讓企業更具體知道其涵蓋範圍。例如，4.2的變更預設密碼，是在設備與保護的面向：6.3的開啟更詳盡的日誌記錄，是在網路與偵測的面向；以及12.1的維護網路邊界清單，是在網路與識別的面向。

同時，鍾澤華還說明了一個重要的觀念，就是要制定優先順序（優先權），才能夠一步步解決問題。簡單而言，CIS CSC可分成基本型、基礎型與組織型，並依據企業規模（Implementation Group）分成IG1、IG2與IG3，他表示，最優先要做的項目是基本型IG1，接著是基礎型IG1、組織型IG1，再來才是基本型IG2，以此類推。

例如，在使用者與保護面向的4.2變更預設密碼，就是該次紅隊演練後首要做到的控制項，然後再陸續達到其他20個控制項的要求。

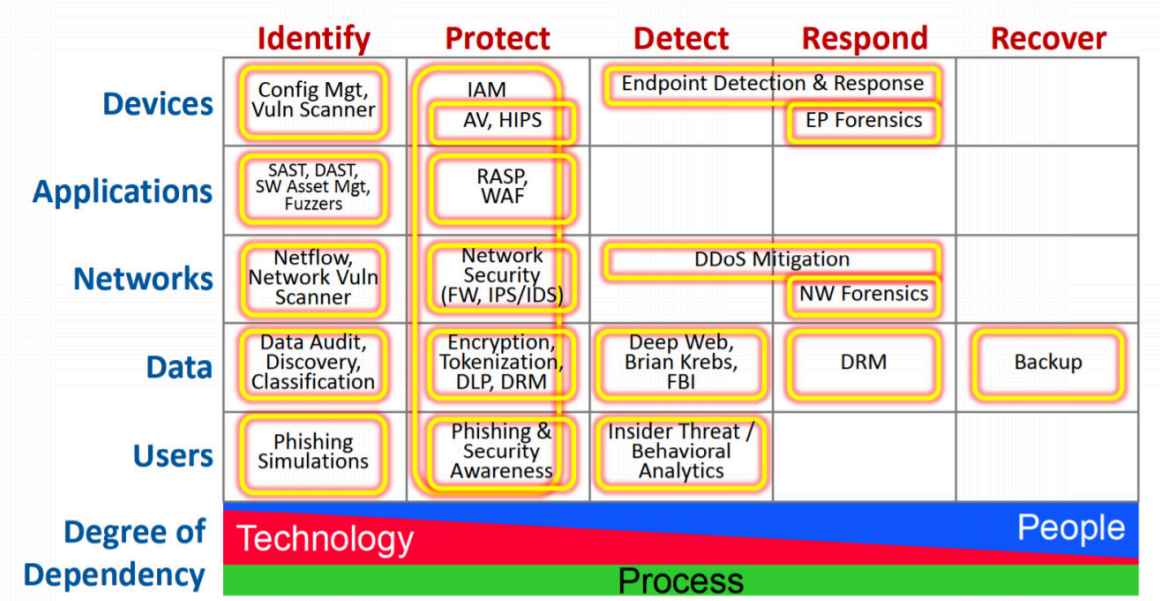
從程序面借助ISO 27001來補強

進一步來看，在控制面之外，還有另一個重要關鍵，是在程序面是否能與控制面做結合，例如，這些控制項是否對應到ISO 27001的項目。鍾澤華表示，當控制措施對應程序層，才能夠更完整思考企業防禦策略的問題在哪裡，例如，套用到Cyber Defense Matrix矩陣後，像是在網路與偵測面向的6.3開啟更詳盡的日誌記錄，從ISO 27001來看將是A16.1.5對資訊安全事故的回應，但此一程序面其實不只是包含於偵測，還有回應、復原。綜合來說，可藉此發現待補強的防禦縱深機制。綜合來看，透過設備、程序與流程面的搭配，才能夠降低弱點被利用的可能性，而上述例子，也就是說明了要從更完整的角度，以檢視面對真實威脅的緩解方式。

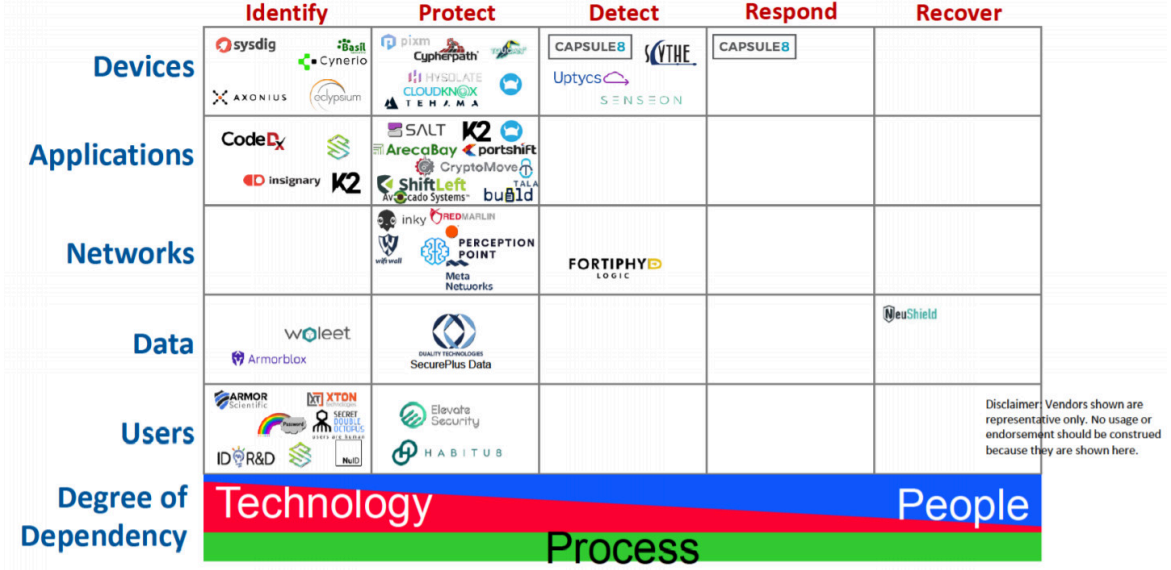
另外，鍾澤華提醒，標準跟框架其實都是一個輔助工具，畢竟框架本身有些要求相當高標，即便國內大企業都不一定是有預算，就能做到，例如，一些控制項要以自動化來完成，因此，企業最好將它們當成思考方針來看待，並依據資源決定要做到什麼程度。

何謂Cyber Defense Matrix？

關於Cyber Defense Matrix的發展，這是2016年美國銀行擔任首席安全科學家的Sounil Yu提出，目前他任職SCVX Corp和FAIR Institute的董事會，並以兼職教授身分教授資訊安全。這個矩陣的橫軸，是NIST CSF的五大類別，而縱軸則是資產類別，可幫助企業理解供應商產品的用途面，並讓整體資安綜合防護的評估更有邏輯與結構。特別的是，這樣的矩陣也漸漸受到業界關注，例如，這個矩陣也納入OWASP當中，而近年RSAC大會上，Sounil Yu也多次在發表相關內容，特別的是，在今年RSAC大會2020現場，會中也提供了Cyber Defense Matrix（CDM）Learning Lab的活動，讓與會者能以互動形式，實際體驗這項矩陣的用法。資料來源：Sounil Yu，iThome整理，2020年9月



對於Cyber Defense Matrix的應用，Sounil Yu提到幾個實例。例如，可藉由矩陣幫助資安防護產品分類，以盤點產品類型對應在矩陣上的範疇，也有類型是跨區塊。以Network Security而言，涵蓋面是網路的保護，而以DDoS Mitigation類型而言，涵蓋是網路的偵測與回應，兩者都是部分的網路面，不能涵蓋到裝置、應用程式、資料與使用者。



另一個應用實例，Sounil Yu在2019年也以當年RSAC新創業者來舉例，用Cyber Defense Matrix將這些業者分類，可以看出該年資安新創的發展趨勢，是聚焦在那個面向。

可借助將CIS CSC融入Cyber Defense Matrix的應用方式，做好控制層的資安管控與規畫

以資安主管負責的控制層為例，將資安框架CIS CSC控制項對應到Cyber Defense Matrix來檢視，例如，圖中淺藍色是基本型控制項、灰色是基礎型控制項，深藍色則是組織型控制項，可讓企業更具體知道各控制項的涵蓋範圍，並能用於制定資安改善優先順序。資料來源：戴夫寇爾，iThome整理，2020年9月

如何透過演練結果調整資安策略？可將發現問題套用到與CDM結合的CIS CSC，再依最低實施要求依序強化

對應攻擊演練結果，企業能夠將資安標準與Cyber Defense Matrix結合使用，以盤點需要強化的設備、控制措施與程序。以上述紅隊演練結果為例，就控制面而言，企業在此案例中，可以利用CIS CSC，先找出需強化的21個控制項，接著標示3大控制群組類型，再依據各控制項的最低實施要求，來決定這項風險企業該補強的先後順序。值得注意的是，這裡建議的順序排列，是從基本型IG1、基礎型IG1、組織型IG1，再來才是基本型IG2、基礎型IG2、組織型IG2，循序做到補強。在此例中，企業第一個動作就是針對「4.2變更預設密碼」先做改善，有順序性的達到目標。資料來源：戴夫寇爾，iThome整理，2020年9月


識別
保護
偵測
裝置
IG3
IG2
IG1
應用程式
網路
資料
使用者
9.2 確保僅有許可的連接埠、協議與服務在運行
18.1建立安全程式碼實務（檔案上傳過濾方式）
14.1 依據敏感性進行網路隔離
14.3 關閉工作站與工作站間不必要的通訊
6.3 開啟更詳細的日誌記錄
12.1維護網路邊界清單
16.1 維護身分驗證系統清單
4.4 使用唯一密碼
4.5 使用多因子認證保護特權帳號存取
4.2變更預設密碼
iThome