2附件一、

中華民國人壽保險商業同業公會

增補契約(十二)

EDR/MDR服務執行計畫書

中華電信股份有限公司企業客戶分公司

中華民國111年XX 月 XX 日

目　　錄

[第一章 資安威脅與端點防護概述 1](#_Toc119583017)

[第二章 MDR服務內容說明 2](#_Toc119583018)

[第一節 MDR服務架構說明 2](#_Toc119583019)

[第二節 監控範圍與服務時間 3](#_Toc119583020)

[一、 監控時間 3](#_Toc119583021)

[二、 監控端點位於網段 3](#_Toc119583022)

[三、 監控的端點範圍與限制 3](#_Toc119583023)

[第三節 前置作業 3](#_Toc119583024)

[一、 專用維運通道 3](#_Toc119583025)

[二、 關聯規則觸發與通報 4](#_Toc119583026)

[第三章 資安事件通報與應變機制 5](#_Toc119583027)

[第一節 事件偵測與通報、調查與應變機制說明 5](#_Toc119583028)

[第二節 事件通報、調查應變機制作業程序 6](#_Toc119583029)

[第三節 事件告警與威脅等級說明 7](#_Toc119583030)

[第四節 專業監控分析與權責分工 8](#_Toc119583031)

[一、 SOC監控工程師 8](#_Toc119583032)

[二、 MDR服務工程師 8](#_Toc119583033)

[第四章 監控通報機制與系統說明 10](#_Toc119583034)

[第一節 告警通報方式說明 10](#_Toc119583035)

[一、 電子郵件通報 10](#_Toc119583036)

[二、 電話通報 12](#_Toc119583037)

[第二節 MDR服務反應時間 12](#_Toc119583038)

[第三節 MDR事件管理入口網站 14](#_Toc119583039)

[第四節 MDR服務月報說明 16](#_Toc119583040)

[第五章 工作項目規劃與交付項目 17](#_Toc119583041)

[一、 工作項目規劃 17](#_Toc119583042)

[二、 文件交付 18](#_Toc119583043)

[第六章 專案執行管理 19](#_Toc119583044)

[第一節 維護、營運：安全管理應變及備援措施 19](#_Toc119583045)

[一、 事件紀錄安全規劃 19](#_Toc119583046)

[(一) 機密性： 19](#_Toc119583047)

[(二) 完整性 19](#_Toc119583048)

[(三) 可用性 19](#_Toc119583049)

[二、 備援機制 19](#_Toc119583050)

[第二節 專案時程規劃 19](#_Toc119583051)

[一、 專案啟動階段 20](#_Toc119583052)

[二、 建置階段 20](#_Toc119583053)

[三、 測試階段 20](#_Toc119583054)

[四、 營運階段 21](#_Toc119583055)

[第三節 驗收計畫 21](#_Toc119583056)

[第四節 服務品質(問題管理、諮詢服務) 21](#_Toc119583057)

[第五節 資安諮詢窗口 22](#_Toc119583058)

圖目錄

[圖 1、MDR威脅偵測應變服務系統架構 2](#_Toc119507455)

[圖 2、MDR偵測與通報、調查與應變處理流程 5](#_Toc119507456)

[圖 3、VMware Carbon Black中控台監控畫面 8](#_Toc119507457)

[圖 4、MDR工程師通報查詢畫面 9](#_Toc119507458)

[圖 5、MDR工程師事件單分析更新畫面 9](#_Toc119507459)

[圖 6、MDR資安事件通報E-mail通報內容（範例） 11](#_Toc119507460)

[圖 7、MDR通報事件彙整 15](#_Toc119507461)

[圖 8、事件報告查詢圖 15](#_Toc119507462)

[圖 9、SOC、MDR月報整合示意圖 16](#_Toc119507463)

表目錄

[表 1、資安事件通報模式與相應變處理 7](#_Toc119507464)

1. 資安威脅與端點防護概述

隨著資訊網路發展成熟，網路帶來了快速與便捷的服務，結合了行動裝置，使得消費者可以不受時間空間的限制，便捷的使用網路進行消費與完成金融手續，刺激更靈活的經濟成長。但網路帶來商機的同時，網路攻擊與機密資料外洩的機會也隨之而來。網路環境安全需要不同面向的資安規劃與實際保護，但大多數公司的資安觀念與做法並未一併提升。與日俱增的線上服務，伴隨著大量服務主機設備與資料存放的主機，但資安防護並完整的涵蓋，進而讓這些設備成為駭客覬覦的目標。普遍的做法是，公司為了保護企業安全與機密，在網路閘道安全領域投入最多的資源作維護，而端點只使用功能單純的防毒軟體保護。忽略了存放資料的端點是駭客終極目標，駭客願意不斷嘗試入侵閘道，只為得到資料。最終的結果是一旦突破了閘道防禦，在企業內部就能夠通行無阻與為所欲為。

為了提供企業組織完整資訊安全保護，除了現有的SOC資安監控中心（Security Operation Center）服務提供閘道與資安設備的監控服務外，更針對端點安全提供了新興的端點保護服務-「MDR威脅偵測應變服務」。此服務提供端點威脅偵測應變服務（Managed Endpoint Detection And Response）服務：服務功能涵蓋了PC電腦與伺服器主機端點的「惡意威脅偵測與防禦」及「資安事件監控與通報」與「專家遠端調查與應變處理」，提供全天候端點即時資安監控服務，提供企業組織的重要端點主機高規格的資安防禦、資安事件通報告警、專家遠端事件應變處理，在資安進階持續威脅APT攻擊與病毒加密勒索威脅發生之前，藉由事前防禦、資安事件中偵測與應變、事後的專家調查，幫助企業精準偵測，快速應變並遏止惡意攻擊。

1. MDR服務內容說明
   1. MDR服務架構說明

中華電信股份有限公司企業客戶分公司與中華資安國際股份有限公司服務團隊(下稱本團隊)提供端點威脅偵測應變系統於中華民國人壽保險商業同業公會(以下稱壽險公會)(使用VMware Carbon Black Endpoint解決方案)，即時監控偵測端點設備執行程序與系統資安狀態，提供即時的資安事件偵測與自動應變的功能。同時提供端點防毒保護（Next-Generation Antivirus, NGAV）能夠偵測與防禦惡意攻擊，快速防禦已知的惡意軟體，能夠即時識別並終止病毒攻擊。同時能以機器學習行為模式的偵測進階持續性威脅（Advanced Persistent Threat, APT）。

本服務主要與SOC資安監控中心資訊整合於同一平台，進行端點MDR端點威脅偵測應變服務與所有設備監控(如：IDS、防火牆、WAF)，統一資安事件通報與事件單追蹤管理，讓管理者專注於統一來源的資安事件風險管理。

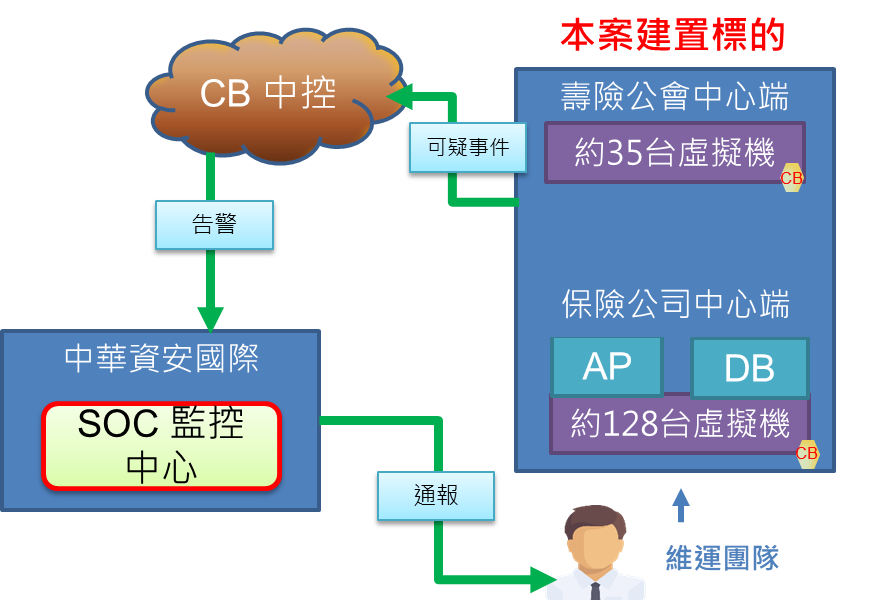


圖 1、MDR威脅偵測應變服務系統架構示意圖

* 1. 監控範圍與監控服務期間
     1. 監控時間

正式監控服務期間從民國112年1月1日至民國116年12月31日止。監控端點位於網段

|  |  |
| --- | --- |
| **網段** | **用途** |
| 10.210.0.0/16  10.211.0.0/16 | 壽險公會中心端 |
| 10.210.0.0/16 | 保險公司中心端 |
| 10.210.0.0/16  10.212.0.0/16  10.213.0.0/16 | 異地備援端 |

監控的端點範圍與限制

本專案將部署壽險公會中心端、保險公司中心端伺服器端點及異地備援端總數至多提供200台主機。

* 1. 前置作業
     1. 專用維運通道

本服務因需要將蒐集的日誌回傳至VMware Carbon Black雲端中控台，並建議以加密HTTPS作為維運通道加密保護，同時亦建議設定防火牆規只開放以下特定URL連線，限制防火牆政策，保障MDR服務日誌拋回與監控與調查通道之安全保障。。

|  |  |
| --- | --- |
| **分類** | **URL** |
| WebUI URL | https://defense-prod05.conferdeploy.net |
| Sensor URL | https://dev-prod05.conferdeploy.net |
| Connector/API URL | https://api-prod05.conferdeploy.net |
| Signature URL | https://updates2.cdc.carbonblack.io |

* + 1. 關聯規則觸發與通報

威脅偵測應變服務的Log轉送至SOC監控中心進行分析後，透過關聯式規則可進一步分析多種惡意攻擊行為，當內部主機連線至惡意程式，將觸發關聯規則會透過系統進行告警通知。

1. 資安事件通報與應變機制
   1. 事件偵測與通報、調查與應變機制說明

MDR威脅偵測應變服務系統，提供「VMware Carbon Black Endpoint」提供精準偵測資安事件的威脅偵測防禦系統。並藉由解決方案提供的國際情資，以高命中、低誤報的即時偵測發現資安事件（Incident）。

在偵測惡意檔案或攻擊時，自動將此事件告警經傳送至SOC監控中心，進行資安事件關聯分析，關聯中華集團相關情資後，由SRM資安風險管理平台(Security Risk Management)即時發出事件告警通報，每一個事件單都會通報資產負責人與MDR服務一~~二~~線工程師 (簡稱MDR服務工程師)與貴公會資產負責人與承辦人。

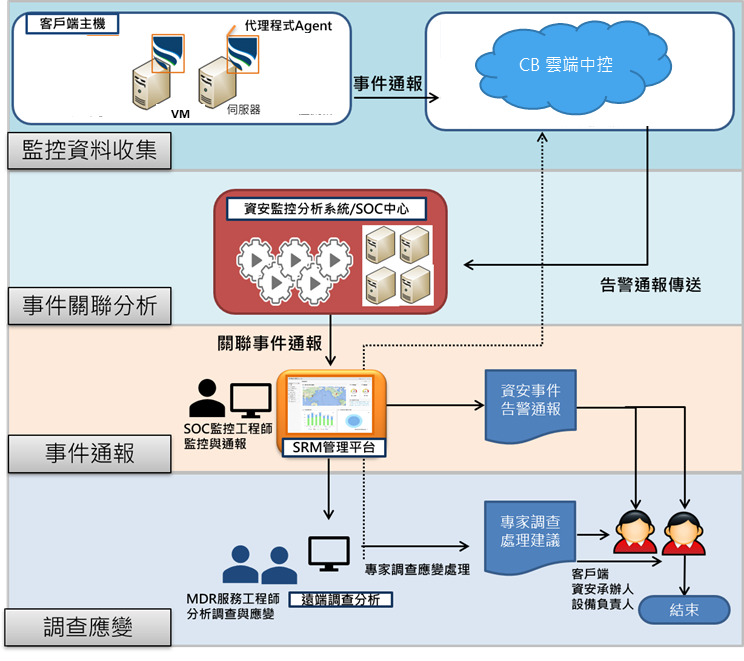


圖 2、MDR偵測與通報、調查與應變處理流程

* 1. 事件通報、調查應變機制作業程序

MDR偵測應變系統偵測惡意行為時，除了產生相應的自動應變處理與立即發送事件通告警，通報SOC監控中心與MDR一線服務工程師，亦會通報告知貴公會承辦人員與資產負責人。公會方可以提出調查需求，由MDR二線服務工程師進階分析未知或可疑惡意行為，並將提供建議與需要應變協助處理。相關的通報、調查應變步驟流程將於下方詳述。

通報處理說明如下：當可疑資安情事出現，中控主機將收集代理程式Agent產生的事件告警通報，傳送至SOC監控中心，藉由關聯分析，確認是否符合被資安分析情資掌握相應特徵(Signature pattern)、樣態(被建檔的威脅入侵指標IOC)的已知資安情事；如病毒威脅、惡意來源的IP\Domain等已知威脅。如果符合，EDR監控軟體將主動阻擋，並將關聯分析後的相關命中情資與該惡意威脅的樣態分析，按威脅的風險等級，藉由Email、簡訊、電話等方式，通報貴公會的承辦人、該發生事件的端點資產負責人、已簽訂該端點對應平台維護合約之團隊維護負責人，資產負責人可進一步追蹤確認此端點檔案或被終止的惡意行為。此項通報亦由SRM資安風險管理平台以事件單紀錄，供資產負責人與承辦人隨後查閱。在此情況下，若公會或維護團隊認為對此一事件有需要加以註記，MDR一線服務工程師亦會於該事件產生的通報事件單上，補充由公會或者維護團隊所提供，該資安事件的相關資料。

若此可疑資安情事，目前情資訊不足以判定為已知的威脅，則EDR監控軟體將主動阻擋，並由MDR一線服務工程師，進行第一階段初階查調，當一線工程師評估後若有必要，將偕同MDR二線工程師進行更專業的鑑識作業。同時也會與資產負責人確認相關資訊細節，例如內部開發程序或相關資訊。一旦MDR服務工程師有初步調查分析結果，將會更新SRM系統上之該事件通報單，供承辦人、資產負責人與維護團隊審閱。

本服務與SOC資安監控中心完整整合，除了MDR服務的偵測防禦、監控與事件管理等能力，監控通報及處理流程，因應可能意外事件發生時，能立即的依所累積的應變處理經驗與機制迅速反應處理。本團隊憑藉著豐富專業能力，落實監控與防禦之功能，依照完整的作業流程分析可疑事件，並且快速通報相關單位與人員。

* 1. 事件告警與威脅等級說明

MDR服務通報的事件告警通報，為端點威脅偵測應變系統(中控主機)偵測端點可疑程序或活動，經過關聯分析，依據情資來判定端點事件內容及風險嚴重等級(含低、中、高風險嚴重等級，簡稱低、中、高風險)，進行初步的資安事件告警通報。

經由SOC監控小組與MDR服務工程師處理，若有必要，亦可以經由分析結果調整為相應的風險等級。例如：藉由情資比對與關聯分析確認為惡意的攻擊來源，因此威脅為已知情資而自動通報為中度威脅風險，而後分析此事件，確認為駭客APT攻擊，將會更新為高風險，並記錄分析結果於SRM資安風險管理平台之事件單。

經以上處理程序，若公會或維護團隊，對上述結果認為應進一步探究，亦可以申請遠端事件調查服務，

表 1、資安事件通報模式與相應變處理

| 通報模式​ | 通報條件 | 系統告警種類 | 應變處理方式 | 類似通報案例 | 風險等級 |
| --- | --- | --- | --- | --- | --- |
| 自動通報 | 已知的病毒或是惡意行為被偵測 | 情資命中告警 (IOC Hit Alert) | 告警並後續追蹤 | 惡意連線C&C對外連線 | 中風險 |
| 專人通報 | 未知或可疑的威脅 | 可疑惡意行為偵測專家已開始調查分析 | 告警，並由中華資安及維護團隊進行處理並回報結果 | APT攻擊駭客橫向移動行為 | 高風險 |
| 無電子簽章的應用程式 | 中風險 |

* 1. 專業監控分析與權責分工

本MDR團隊將憑著專業技術及進階分析所有可疑威脅攻擊。這些事件的種類及嚴重等級藉由考慮許多不同的準則來判定，例如：攻擊來源、目的、方向以及客戶對資訊安全的標準。SOC工程師負責日常監控中心的維運工作，而MDR工程師負責事件分析調查，共分成二線維運機制：

* + 1. SOC監控工程師

SOC人員於事件通報流程中負責通報事件確認、每日監看安全事件集中分析平臺與中控主機，將關聯分析後的資安事件以及軟硬體設備異常狀況通報給MDR服務工程師，MDR服務工程師將登入VMware Carbon Black中控台進行確認及資安事件分析。VMware Carbon Black中控台監控畫面如下圖所示。

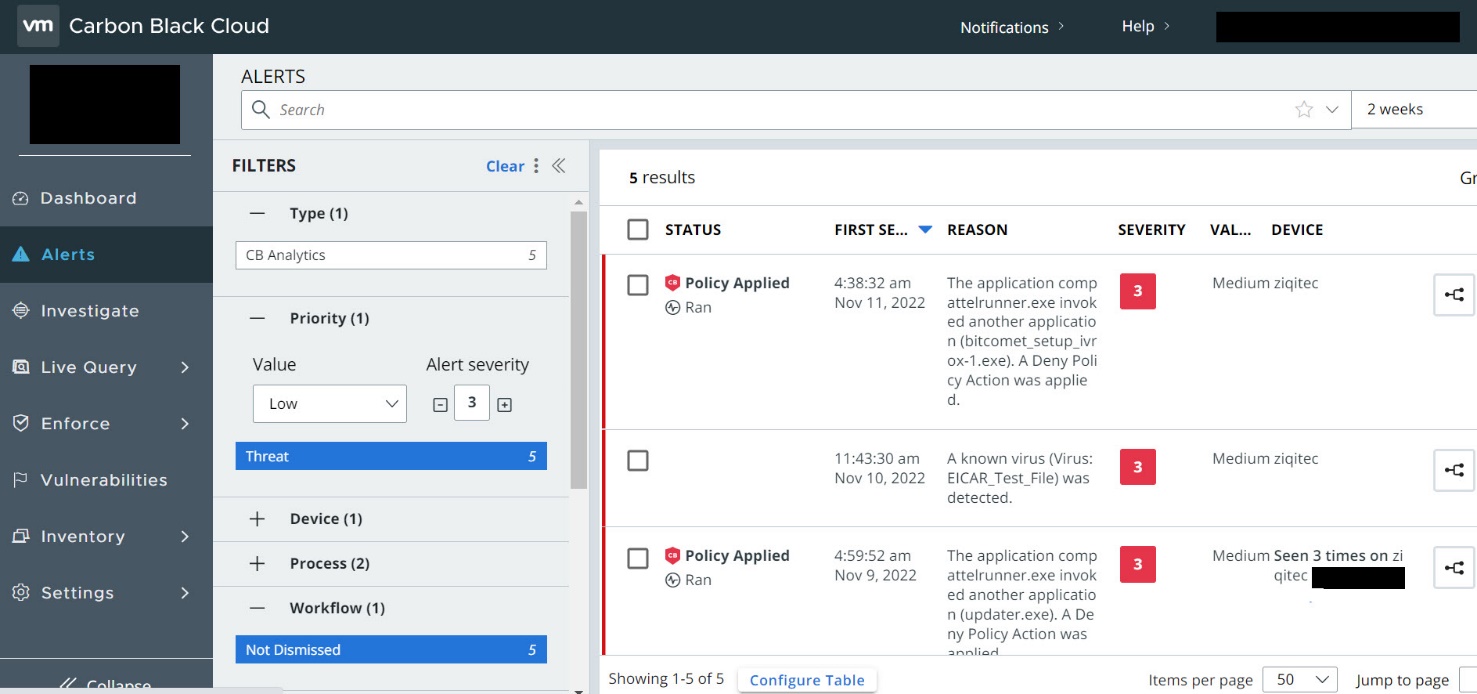


圖 3、VMware Carbon Black中控台監控畫面

* + 1. MDR服務工程師

事件通報流程中負責監看事件單處理系統與MDR監控與偵測，以及審核一線人員通報之事件單，經由事件單內容查看事件內容與網路拓樸，瞭解事件源由，並且提供一線人員所需的各項協助，包括：事件的分析、追蹤處理及客戶諮詢。二線人員通報及查詢畫面如下圖所示。

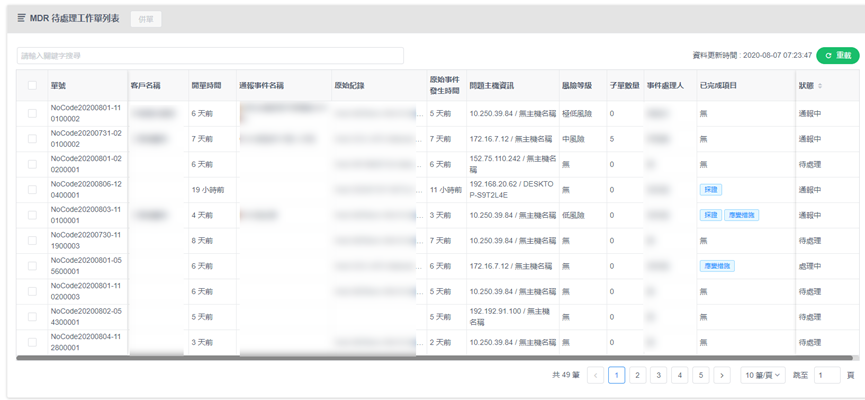


圖 4、MDR工程師通報查詢畫面

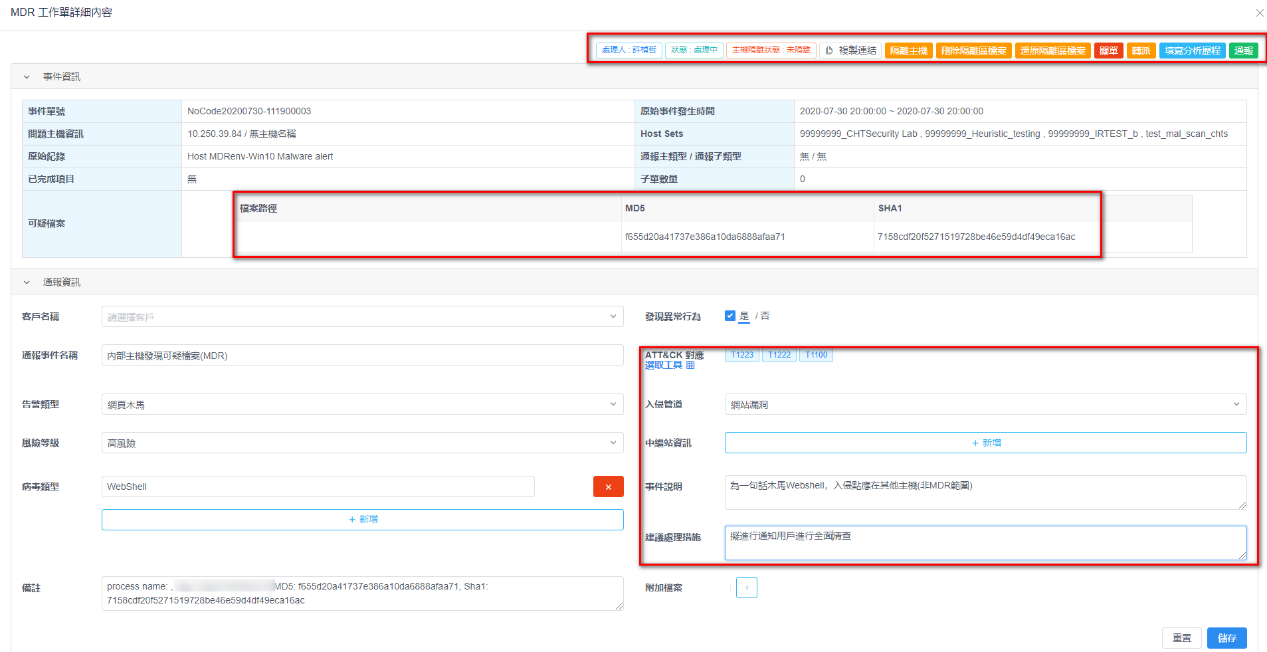


圖 5、MDR工程師事件單分析更新畫面

MDR工程師負責全球最新資安事件的發生原因分析、鑑識入侵管道、根除與復原方式以及最新駭客手法等技術研究。

1. 監控通報機制與系統說明
   1. 告警通報方式說明

SOC一線資安專業人員將針對本專案所佈署之資安設備所產生的告警訊息進行7×24全天候無休之即時監控及預警通報，透過與客戶密切合作，人員將採取快速、專業的回應幫助客戶在潛在資訊損失發生之前做好防禦及入侵工作。

有關資安事件通報方式及對象層級如下表：

|  |  |
| --- | --- |
| **通報方式** | **通報方式** |
| 已知威脅事件  (自動通報) | （第一聯絡人）  傅駿勳  jeffrey648@liaroc.org.tw  0988-293-213  02-2561-2144#678  （第二聯絡人）  陳乙棋  yichi@liaroc.org.tw  0938-486-520  02-2561-2144#680 |
| 專人通報 | （第一聯絡人）  傅駿勳  jeffrey648@liaroc.org.tw  0988-293-213  02-2561-2144#678  （第二聯絡人）  陳乙棋  yichi@liaroc.org.tw  0938-486-520  02-2561-2144#680 |

依資安事件等級之電子郵件、電話之通報對象如下：

* + 1. 電子郵件通報

|  |  |
| --- | --- |
| **通報模式** | **通報對象** |
| 已知威脅事件  (自動通報) | （第一聯絡人）  傅駿勳  jeffrey648@liaroc.org.tw  0988-293-213  02-2561-2144#678  （第二聯絡人）  陳乙棋  yichi@liaroc.org.tw  0938-486-520  02-2561-2144#680 |
| 專人通報 | （第一聯絡人）  傅駿勳  jeffrey648@liaroc.org.tw  0988-293-213  02-2561-2144#678  （第二聯絡人）  陳乙棋  yichi@liaroc.org.tw  0938-486-520  02-2561-2144#680 |

事故觸發後將發送事故通報內容電子郵件，範例如下圖所示。



圖 6、MDR資安事件通報E-mail通報內容（範例）

包含多項基本資訊與事件資訊：

* 權責單位
* 事件單號
* 目前流程
* 派單時間
* 問題端資訊
* ATT&CK Tactics
* ATT&CK Techniques
* 通報事件名稱
* 風險等級
* 告警類型
* 中繼站位址
* 病毒類型
* MD5
* SHA1
* 入侵管道
* 事件說明
* 建議處理措施

電話通報

| **通報層級** | **通報對象** |
| --- | --- |
| 高風險事件 | * 循環通知到第一位即可   第一聯絡人🡺第二聯絡人🡺第一聯絡人……   * 第一聯絡人   姓名：傅駿勳  行動電話：0988-293-213  市內電話：02-2561-2144#678   * 第二聯絡人   姓名：陳乙棋  行動電話：0938-486-520  市內電話：02-2561-2144#680 |

* 1. MDR服務反應時間

MDR擁有每日24 小時全年無休之SOC專職輪班人員監控設備運作及完整的MDR服務監控流程管理制度，落實執行所有控管與改善措施。MDR服務反應時間如詳細內容請參考如表2。

表 2、MDR服務資安事件反應（應變回覆）時間說明表

|  |  |  |  |
| --- | --- | --- | --- |
| **服務功能** | **描述** | **服務反應時間** | **說明** |
| 威脅偵測應變 | 情資自動偵測 7x24監控通報 | 7D\*24H (資安事件通報) | 系統偵測惡意事件後，系統立即自動阻止後續惡意事件，並馬上發出警告給監控人員，資安承辦人與設備負責人也將在10分鐘內收到相應的事件通報信件(有可能因網路延遲而超過10分鐘收到通報信件)。 |
| 專家遠端調查應變 | (1)專家遠端事件調查應變  (2)威脅主動獵捕 | 5D\*8H (專家調查結果回報 ) | (1)系統偵測可疑事件後，系統立即發出通報給監控人員。調查人員將於貴公會同意下，啟動遠端資安事件調查與協助貴公會應變處理。週末與連續假日，仍有7\*24監控系統與通報事件。  (2)當國際發生重大的資安事件(如Log4j)，貴公會可主動提出調查需求，請調查人員清查EDR監控主機可疑項目。 |

* 1. MDR事件管理入口網站

MDR服務監控與事件紀錄管理，將使用「SRM資安風險管理平台」提供詳細的資訊，將資安監控事件進行開單、通報、處理及追蹤，並提供事件之歷史資料查詢。

並提供多組帳號供貴公會用，監看資訊包含：每日資安事件、專屬風險指數、風險趨勢分析、歷史事件報表及事件統計分析等整合性資訊，藉由以上整合資訊協助客戶全盤掌握資安狀態，專注於高風險資安事件與處理進度。

|  |  |  |
| --- | --- | --- |
|  | **平台功能項目** | **內容說明** |
| 1 | 提供5組登入帳號供機關使用 | 可以提供多組帳號供機關登入使用。將依照本案的建議提供四種等入瀏覽管理權限：   1. 系統管理員。 2. 資產負責人。 3. 稽核人員。 |
|  | 平台功能與介面 | 內容說明 |
| 2 | 即時資安案件檢視及分析 | 最新資安案件須於通報後30分鐘內即可查詢。 |
| 3 | 歷史資安案件查詢及統計 | 資安事件經通報後即可在此平台針對時間區間進行查詢。 |
| 4 | MDR服務事件通報作業 | 本平台會在首頁顯示相關資安預警訊息，也會透過EMAIL方式將訊息寄送給主要窗口。 |
| 5 | 資安案件處理狀況追踪 | 可以針對過去的案件進行查詢。 |
| 6 | 資安預警情報 | 國內外資訊安全威脅通報資訊。 |

SRM資安風險管理平台事件管理如下圖7、8所示，更詳細的操作使用於MDR服務使用者操作手冊中說明：

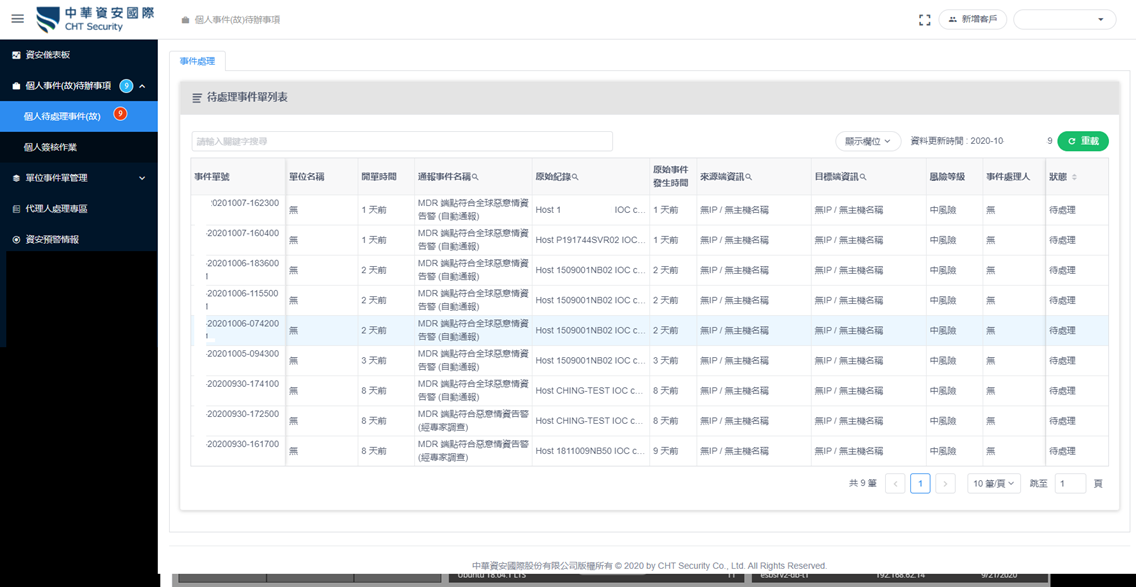


圖 7、MDR通報事件彙整



圖 8、事件報告查詢圖

* 1. MDR服務月報說明

資安監控服務機制建立開始運作次月起，依需求書要求每月15日前，將前1 個月MDR資安事件整合於SOC月報。報告內容是依據前一個月 MDR所監控、記錄之事件，做統計與建議說明，以Word 檔案格式提供，除了各項可疑攻擊事件外，也將遇到之問題及改善之建議一併提出，並與貴公會通討論，分析撰寫之內容可讓維運人員瞭解事故的發生與建議，以利客戶持續提升資通安全防護能力。每月彙整之報表包含下列各類統計資料：

* 資安事件(故)說明
* 建議改善項目

一張含有 文字 的圖片

自動產生的描述

圖 9、SOC、MDR月報整合示意圖

1. 工作項目規劃與交付項目
   * 1. 工作項目規劃

|  |  |  |
| --- | --- | --- |
| **階段** | **內容** | **時程** |
| 專案啟動會議 | * 專案服務執行計畫書 | 111年10月31日前完成。 |
| 第一階段專案啟動階段 | * 網路架構確認。 * 需求訪談與資產盤點。 * 說明專案進行方式、建置時程及配合事項。 | 111年11月5日前完成。 |
| 第二階段  建置階段 | * EDR/MDR間防火牆規則設定。 * 完成端點EDR軟體部署及連線報到。 * 日誌拋送到中華資安SOC資安監控中心並完成設定啟用。 | 111年12月10日前完成。 |
| 第三階段  測試階段 | * MDR監控系統上線前測試：   觀察LOG收容狀況及規則觸發狀況，再予以調校。 | 111年12月20日前完成 |
| 第四階段  營運階段 | * 提供完工報告書。 * 正式啟動MDR監控及觸發規則上線。 * 自上線日次月起，每月15日前以電子檔提供整合上個月MDR資安事件之SOC月報 | 112年1月1日正式上線，為期五年的監控通報。 |

* + 1. 文件交付

| **工作項目** | **內容** | **時程** |
| --- | --- | --- |
| 專案服務執行計畫書 | 專案服務工作計畫書包含專案服務內容規劃、執行方式說明、專案小組成員名單、服務時程規劃與交付文件時程。 | ￭111年10月31日前提供。 |
| 完工報告書 | 內容包含安裝完成以後，端點測試接通的成果，功能模組測試是否正常、事件啟動程序測試結果。 | 112年1月1日前提供。 |
| EDR5年授權證明書 | VMware Carbon Black原廠授權證明書 | 112年1月1日前提供。 |
| 資安監控服務月報告 | 每月15日前，以電子檔方式提供上個月資安監控服務報告 | ￭**上線日起**，為期五年的監控通報，每月15日以前交付。 |

1. 專案執行管理
   1. 維護、營運：安全管理應變及備援措施
      1. 事件紀錄安全規劃

本專案執行期間收集貴公會伺服器等重要設備之事件紀錄，對於資料有著嚴密的保護，以維護貴公會資訊之機密性（Confidentiality）、完整性（Integrity）、可用性（Availability）。

* + - 1. 機密性：

本團隊規劃於貴公會與CHT Security SOC資訊安全監控平台各元件之間傳送事件紀錄時，連線通道採用SSL加密保護，以確保傳送資料不會遭受惡意的竊聽或竄改。

* + - 1. 完整性

存放於SOC資安監控中心的資安事件，以雜湊函數(Hash function)為主的驗證機制，以確保存放資料的完整性。

* + - 1. 可用性

中控主機會將發生資安事件的事件通報，藉由傳送回CHT Security SOC資安監控中心系統程式採RAID磁碟備援，日誌資料儲存於NAS儲存系統RAID 磁碟備援陣列，預防單一硬碟故障造成資料遺失，並且規劃儲存系統部分空間提供系統程式與檔案備份，提高可用性。

* + 1. 備援機制

本專案中控主機系統建置於VMware Carbon Black雲端機房，具備高可用性及異地備援機制。

* 1. 專案時程規劃

本團隊將專案時程規劃分為4個階段執行本專案：專案啟動、建置階段、測試階段、營運階段~~與專案結案及交接~~，本團隊專案期程規劃如下:

* + 1. 專案啟動階段

為能於得標後儘速進行專案工作，規劃於取得貴公會訂單後舉行專案動會議，確認雙方專案團隊成員、連絡窗口、專案進行方式及雙方配合事項等。

於專案需求訪談會議時確認貴公會網路架構及服務細節：

* + - * 1. 內部網路架構細節
        2. 本專案範圍內資安防護現況、主機數量及相關資訊：

資安設備及伺服器端資產管理現況

伺服主機及IP位址分配表

網站IP與網址資訊

通報窗口及聯絡資訊

* + - * 1. 專案進行方式、建置時程及配合事項
    1. 建置階段

依與貴公會所協調確認之建置時程及完成日期，安排人力同時開始進行整體事件紀錄收容機制之建置，以及各項專案服務之執行，如期完成各項專案工作。

* + 1. 測試階段

待整體軟硬體設備及服務建置完成後，本團隊將與貴公會相關同仁進行測試，檢查各項服務能順利運作，並且適時做關聯規則調整，提升服務品質。所有工作時程及交付項目，將依本專案需求說明書所訂之各期程履約。

* + 1. 營運階段

開始營運後，依據本專案需求進行各項資安防護、監控、通報及應變處理服務，並確保各項服務品質，以達成資安共契服務規範之SLA。

* 1. 驗收計畫

本服務案需於民國111年12月31日前完成本案EDR軟體部屬及設定並通知甲方進行驗收作業。

針對本服務案訂定驗收所需交付之工作項目，如下表所示，如期、如質、如量完成交辦項目。

|  |  |  |  |
| --- | --- | --- | --- |
| 驗收項目 | 驗收內容 | 是否符合 | 備註 |
| 完工報告書 | * 確認已報到Server主機符合部署清單。 | 是□ 否□ |  |
| * 確認端點定期回報機制。 | 是□ 否□ |  |
| * 事件單發送測試。 | 是□ 否□ |  |
| 軟體授權證明 | * EDR 5年軟體授權證明。 | 是□ 否□ |  |

* 1. 服務品質(問題管理、諮詢服務)

為了保證本專案之品質，本團隊除將指派具有相當經驗及良好素質與訓練的人員參與本專案，成立專案組織，研訂工作計畫開始，至產品交付驗收及開始維運管理，凡建置、測試、文件交付等之各個過程，均納入品質控管程序中。

貴公會現有資安閘道設備如APT (Lastline)、WAF(F5 i2600)及FortiGate防火牆相關日誌已收容到CHT Security SOC資安監控中心進行監控，並將日誌內容依照監控的標的進行規則撰寫，針對重要資安日誌發送告警，並進行事後分析，建立第一道資安防禦機制。

然而安全強度取決於最弱一環，當資安閘道設備存在零時差漏洞(Zero-Day Vulnerability)，或企業內部員工遭受社交工程攻擊時，都可能遭受駭客利用，突破資安閘道設備防禦，導致企業內部機敏資料被竊取及加密，而VMware Carbon Black EDR軟體可強化端點防護避免入侵，在偵測惡意檔案或攻擊時，自動將此事件告警經傳送至CHT Security SOC資安監控中心，形成第二道資安防禦機制。

當資安事件發生時，貴公會專屬之SOC、MDR及鑑識服務技術同仁，將協同合作，利用鑑識情資與遠端調查分析，直接提供明確的資安事件分析通報與應變建議。且本專案MDR服務與本團隊CHT Security SOC資安監控中心資訊整合於單一資安管理平台(Security Risk Management,簡稱SRM資安風險管理平台)，進行端點MDR端點威脅偵測應變服務，統一資安事件通報與事件單追蹤管理，讓管理者專注於統一來源的資安事件風險管理，建構起第三道資安防線。

透過上述三道資安防護機制，有效加強防禦縱深與偵測點，並導入監控及應變機制，中華電信團隊共同為保護貴公會關鍵資源區而努力。

* 1. 資安諮詢窗口

本案提供7×24全年無休一線諮詢服務受理窗口，窗口資訊如下：

CHT Security SOC

諮詢號碼：02-23443693

服務信箱：hinetsoc@cht.com.tw

本案5×8二線資訊安全諮詢窗口資訊：

| 職稱 | 姓名 | 辦公室電話 | e-mail |
| --- | --- | --- | --- |
| 專案經理 | 姜廷儒 | 02-2343-1628#8005 | steven.chiang@chtsecurity.com |
| 專案經理 | 林蓮蒂 | 02-2343-1628#8047 | lanti@chtsecurity.com |
| MDR監控服務  聯絡窗口 | 莊友豪 | 02-2343-1628#3048 | andyet921@chtsecurity.com |