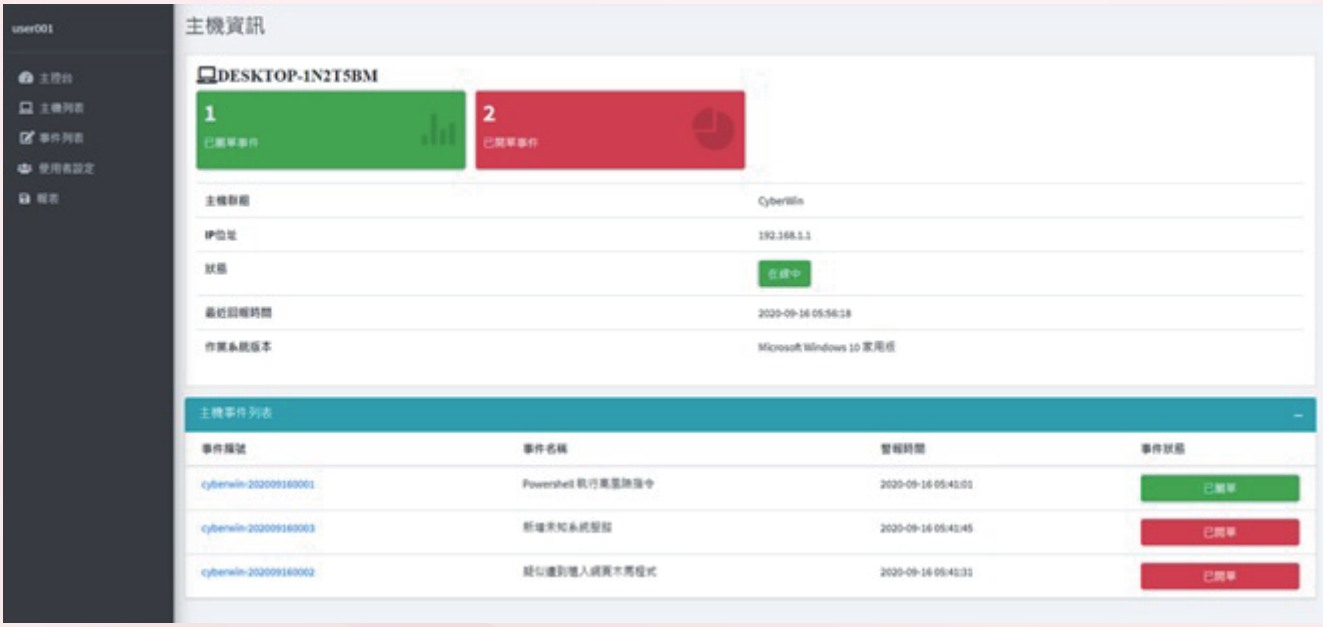
資安威脅偵測管理系統/使用授權

資安威脅偵測管理系統(MDR)解決傳統資安事件處理的缺點，主動收集端點系統活動資訊，達到隨時收集與鑑識的能力。加上網路攻擊的早期階段，因為攻擊者擁有的資訊與權限相對稀少，所以攻擊的手段相對單調容易辨識。

本系統可讓任何疑似攻擊的系統活動，在早期階段就被分析並辨識正常與否。越早開始進行處理，就可以越有效的降低損失。



系統

- MDR服務
- 網路威脅獵捕
- 資安事件處理
- 定期報告

特色

●即時檢測端點威脅

資安攻擊日趨針對性及持續性。

●持續性的檢測、監控及分析

傳統一次性或定期檢測方式，常出現時間差等問題，沒辦法在事件發生擴大前及時發現更無法進行追蹤。

●資安事件回應及遠端處理

資安事件具時效性及迫切性，需在災損出現或擴大前予以及時處理。

資安威脅偵測(MDR)	V.S.	傳統防禦架構
即時分析與處理	處理時效	等到事後才處理
主動式威脅獵捕分析	分析模式	被動式等待資料整合
高度自動化的分析與處理服務	自動化程度	需大量人力介入處理
本土全域聯防及情資即時更新	情資整合	各組織自行處理或購買國外情資
可鎖定未知的攻擊手法	處理範圍	主要偵測已知的攻擊方式
僅需確認處理結果	管理負擔	需全程參與並負擔對應工作

本模組除管理端外，使用端必須再購買使用授權

經銷商蓋章

華麗得股份有限公司
Brecioso Co., Ltd.
TEL：02-89235035
service@brecioso.com