CIMCOR

技術摘要

當您的企業或代理商需要確保您的IT基礎設施的完整性和法規遵循時，請找CIMTRAK

CimTrak是幫助全球組織與政府機構維護其關鍵IT資產的安全性、完整性、法規遵循與可用性的領導者。憑藉行業領先創新的成功記錄，CimTrak始終如一地將新想法推向市場。

特色

- 深入了解系統的狀態
- 提高形勢的感知能力
- 減少事件反應時間
- 改善安全狀況
- 降低補救成本
- 支援連續監控
- 有助於法規遵循工作
- 易於使用
- 設定簡單
- 動態威脅反應
- 自動復原功能

為什麼選擇CIMTRAK？

包括眾多財富500強公司的各種規模的組織依賴於CimTrak，為用戶提供功能齊全的檔案完整性監控file integrity monitoring解決方案，易於安裝、設定與管理，有別於許多FIM解決方案相關的昂貴預算與複雜性。CimTrak獨特的SmartFIM™技術意味著您可以在更短的時間內完成更多工作，從而為您的組織節省時間和金錢。 在世界一流的支援團隊的支援下，CimTrak用戶可以放心，讓他們的系統始終處於穩定的狀態。

跨越您的IT環境偵測異動

透過涵蓋您的伺服器、網路設備、關鍵工作站、POS銷售點系統等，CimTrak可以覆蓋您的基礎設施。是單一收集點的設定與管理解決方案，報告可能影響運營、安全性與法規遵循的變更。

異動發生時的即時通知

CimTrak可以讓您深入了解您的IT環境中正在發生的情況，透過即時了解異動，您可以隨時了解關鍵IT基礎設施的狀態。

自動修正措施

能夠快速反應可能導致系統崩潰及業務停滯的異動是至關重要的，CimTrak讓您能夠立即採取自動操作來完全修復或防止سم ؟ 。

識別出良好的異動

當發生意外異動時，能夠辨別異動檔案是好還是壞是非常重要的，透過CimTrak與惡意軟體分析引擎malware analysis engines的強大整合，現在可以快速、簡單地執行這種困難且經常令人沮喪的分析任務。

提供所有檔案的異動

CimTrak為您提供有關IT環境的異動與所採取措施的完整報告。 此完整報告允許追蹤與驗證異動，稽核與法規遵循報告以及執行級別報告。CimTrak還可以輕鬆地將收集的變更資訊匯出到許多企業和政府機構中，包括安全性的各種報告與警報工具。

www.cimcor.com

了解更多產品資訊，請洽:台灣地區代理商 商丞科技股份有限公司 (02) 2914-8001

CIMTRAK如何運作

CimTrak透過檢測檔案與設定的新增、刪除、修改與讀取來運作。在初始設定時，CimTrak拍攝您需要監控的檔案與設定的“快照“snapshot”，它建立檔案與設定的加密hash，並將它們安全地儲存在CimTrak主儲存庫Master Repository中，建立一個已知的良好基線Master Repository。從那裡CimTrak從各種CimTrak代理程式agents與模組modules接收資料。當收到的模組與特定檔案與設定加密hash cryptographic hash不一致時，意味發生了異動，CimTrak 將根據 CimTrak的設定方式採取措施。通過SMTP和系統日誌發送警報，並根據需要進行即時或手動異動復原。

CIMTRAK MASTER REPOSITORY主儲存庫

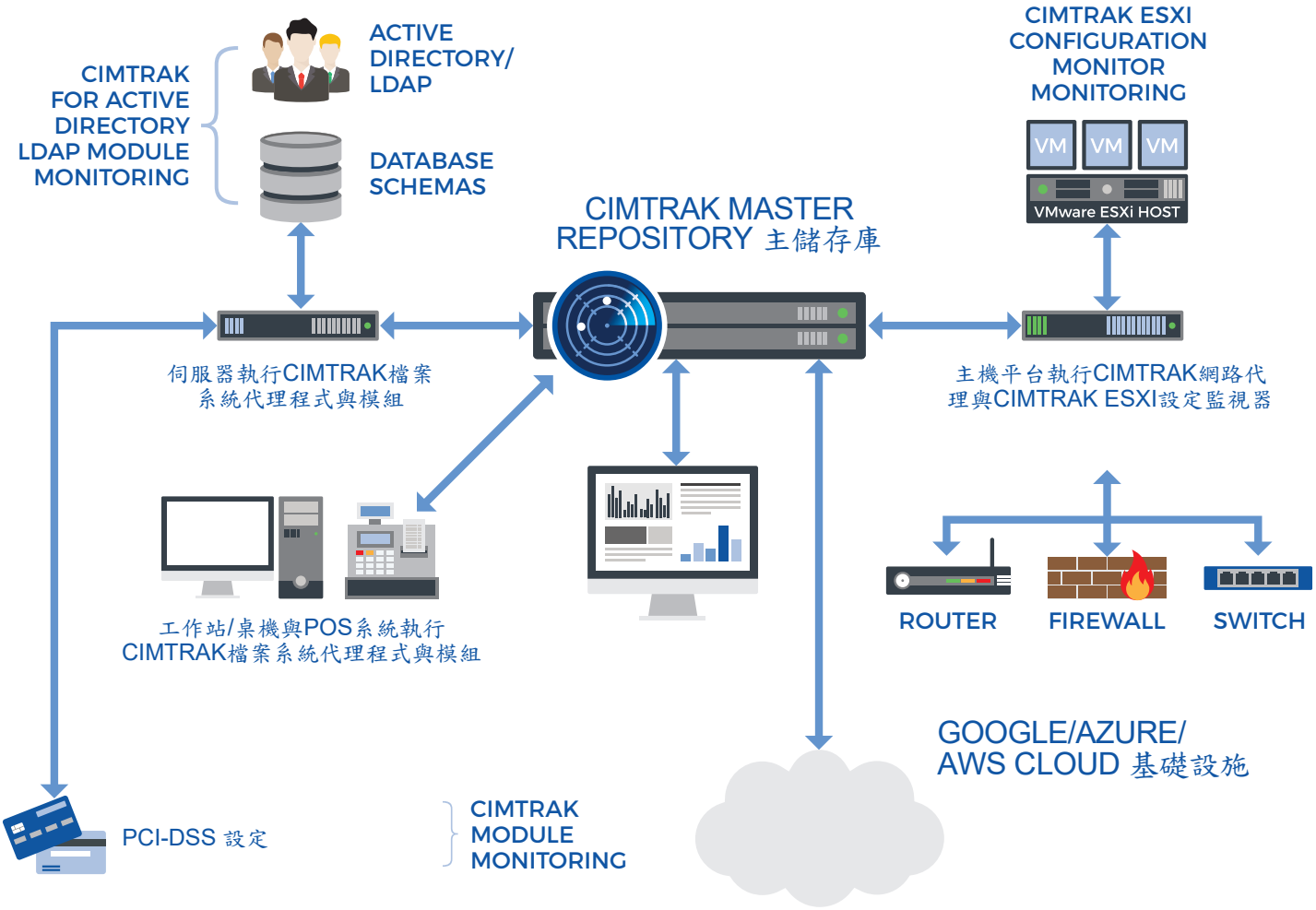
安全地儲存檔案與設定，並執行比較以偵測異動。

CIMTRAK AGENTS/MODULES 代理程式與模組

適用於IT環境中的各種元件與應用程式，並將檔案與設定發送回CimTrak 主儲存庫進行比較。

CIMTRAK MANAGEMENT CONSOLE 管理控制台

CimTrak管理控制台支援多個用戶以及多租戶Multi-Tenant 檢視。



CIMCOR

CimTrak產品商標為 Cimcor公司所有

了解更多產品資訊，請洽:台灣地區代理商 商丞科技股份有限公司 (02) 2914-8001

CIMTRAK的操作模式

LOG 日誌

Cimtrak 記錄被監視的系統與應用程式的所有異動，並可進行分析和報告。

UPDATE BASELINE 更新基線

CimTrak儲存發生異動時檔案與設定的增量“快照”“incremental snapshot”，此功能分析在快照與先前的基線之間異動並允許隨時進行異動復原。

RESTORE 復原

CimTrak具有偵測到異動時立即採取反轉異動行動的能力，可有效地允許系統“自我修復”self-heal，CimTrak是唯一具有這種強大功能的完整性工具。

DENY RIGHTS 拒絕權限

拒絕任何檔案異動，由於CimTrak使用本地系統帳號 local system account 執行，因此無論使用者具有什麼存取權限都不被允許異動檔案，如檔案更改、刪除或新增，沒有其他完整性工具提供這種進階功能。

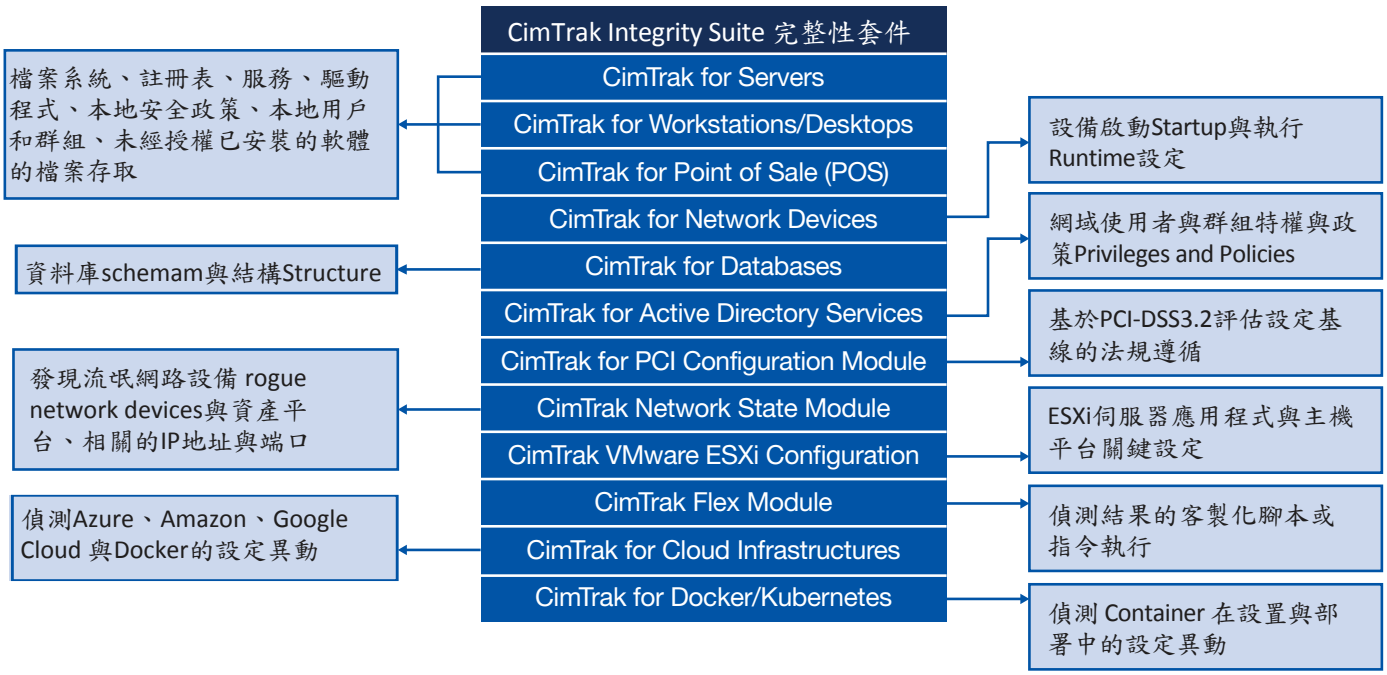
值得注意的是，CimTrak在使用各種模式時可以提供很大的靈活性。您不會被限定每個檔案或設定只使用一種模式。
相反的，您可以根據異動類型選擇CimTrak應執行運行的模式，例如您可能希望簡單地記錄特定檔案的異動，但如果該檔案被刪除，可以將檔案恢復。

CIMTRAK 是安全的

基於政府客戶的嚴格需求，CimTrak已獲得通用標準EAL Level 4 +認證，該認證是商業軟體產品的最高政府認證。此外CimTrak加密模組已通過認證並符合美國聯邦資訊處理標準（FIPS）140-2 Level 2要求，並在美國國防部認證的產品列表中列出，這是IT安全產品的精英名單。

此外，您的關鍵資料是安全的，CimTrak在元件之間的所有傳輸都完全加密，CimTrak主儲存庫以壓縮與加密的形式儲存您的檔案或設定沒有其他的完整性和法規遵循工具有搭配這些嚴格的保護措施來保護您的資料。無論您是政府機構還是商業企業，您都可以放心，因為CimTrak是安全的！

CIMTRAK 監測什麼



CIMCOR

CimTrak產品商標為Cimcor公司所有
了解更多產品資訊，請洽:台灣地區代理商 商丞科技股份有限公司 (02) 2914-8001

CIMTRAK FOR SERVERS

能夠在大多數作業系統上提供即時偵測異動能力，CimTrak提供您即時偵測與警報功能。另外CimTrak監控安全策略、系統設定、驅動程式、安裝的軟體、服務、使用者與群組。進一步CimTrak監控您的IT基礎設施的健康狀況，包括 CPU利用率、記憶體、磁碟空間與 網路利用率，立即提醒您任何問題。 CimTrak甚至可以偵測當檔案被打CimTrak 使用最小CPU資源與網路頻寬為您的IT環境提供最完整的整合，且不會影響您的效能。

CIMTRAK FOR WORKSTATIONS/DESKTOPS

CimTrak for Workstations / Desktops可以監視具有特定功能或執行某些關鍵應用程式的工作站與桌機。這些存在於許多環境中，包括飯店、餐廳、能源與製造業。 CimTrak for Workstations / Desktops允許您監視與CimTrak for Servers相同的所有項目，但是將規格縮小以滿足較小機器的需要，包括使用最少的系統和網路資源。

CIMTRAK FOR POINT OF SALE (POS) SYSTEMS

CimTrak for Point of Sale Systems在您的支付卡環境中增加了POS系統的支援。作為您的支付卡基礎設施不可或缺的一部分，保護這些系統有助於確保客戶的支付卡資料的安全性。

CimTrak為您提供最完整的支援，在保護支付卡環境，保持他們的安全與穩定的完整性狀態。

CIMTRAK FOR NETWORK DEVICES

CimTrak for Network Devices 偵測並提醒您關鍵網路設備上的設定異動，包括路由器、交換機和防火牆。 由於這些設備通常是進入您網路的關口，無論是惡意還是意外的設定異動都可能是非常有問題。CimTrak甚至可以立即恢復SNMPv3網路設備上異動的設定。

CIMTRAK FOR DATABASES

CimTrak for Databases為您的IT環境增加了另一層安全性。支援包括Oracle、IBM與Microsoft在內的主要平台，CimTrak可確保您的關鍵資料庫的設定、用戶角色、權限以及存取設定不會偏離其已知的受信任狀態。透過使用CimTrak for Servers，您可以進一步監視資料庫應用程式，以獲取可能影響營運的關鍵資料庫異動。

CIMTRAK FOR ACTIVE DIRECTORY/LDAP

CimTrak for Active Directory / LDAP監視目錄服務，以查找對象、屬性和架構的偏差。大型環境可能遭受監視外的改變。由於採用分層設計，意外的異動可能僅限於單個實體，例如增加新帳號、或者拒絕服務 Denial of Service。 CimTrak提供在發生此類偏差時快速偵測與警報所需的意識。

CIMTRAK PCI CONFIGURATION MONITOR

CIMTRAK PCI CONFIGURATION MONITOR評估PCI環境中的伺服器、工作站與POS系統上的設定。 透過根據既定標準檢查您的設定，您可以確定系統是否符合PCI-DSS要求。 CimTrak 提供遵循法規要求的詳細報告，以便您可以快速讓系統進入法規遵循狀態，然後CimTrak確保偵測到任何後續設定異動將立即提醒您。這確保您的關鍵PCI設定始終處於符合法規與安全的狀態。

CIMTRAK VMWARE ESXI CONFIGURATION MONITOR

The CimTrak ESXi Configuration Monitor監視關鍵核心VMware ESXi設定，例如用戶/主機存取權限、Active Directory領域、網路設定、整合的第三方工具與進階使用者設定。由於VMware ESXi hypervisors虛擬機管理程序通常執行許多虛擬機，因此意外或惡意更改可能會迅速削弱組織的IT基礎設施。 CimTrak ESXi Configuration Monitor設定監視器使您能夠主動保護關鍵ESXi應用程式並確保操作的安全性和連續性。

CIMTRAK FLEX MODULE

CimTrak Flex Module允許監視寫入指令的應用程式與腳本的輸出，例如ipconfg / ifconifg網路設定、防火牆設定、安全增強的Linux設定狀態等。 CimTrak Flex Module還可用於監控實體硬體狀態，如SAN運作狀況、以及元件與資源可用性。 此外，它允許在IT環境中快速開自行定義的應用程式監視工具。通過偵測對腳本/應用程式輸出的任何異動，可以立即提醒和反應偏差。自動監視與分析自行定義腳本或指令執行script or command line execution的能力，簡化IT操作，使人員能夠專注於更緊迫的問題。

CIMCOR

了解更多產品資訊，請洽:台灣地區代理商 商丞科技股份有限公司 (02) 2914-8001

CIMTRAK FOR CLOUD INFRASTRUCTURES

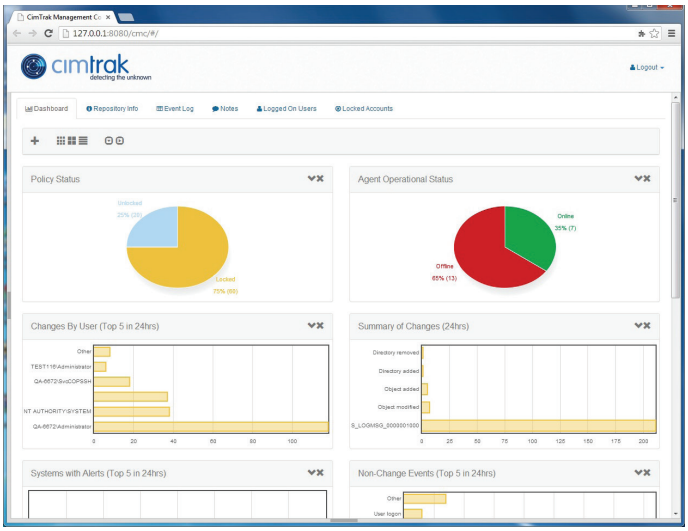
CIMTRAK FOR CLOUD INFRASTRUCTURES提供了一種簡單的方法來了解何時配置新的雲端伺服器、或者伺服器配置設定、虛擬防火牆規則、虛擬網路等發生了異動。CimTrak for Cloud Infrastructures支援Google Compute Engine、 Azure與Amazon AWS 、CimTrak for Cloud Infrastructures允許您監控Guest作業系統之外的雲端基礎設施發生的所有異動。

CIMTRAK FOR DOCKER/CONTAINERS

CimTrak for Docker/Kubernetes可幫助管理員了解容器Container設定何時發生異動、新容器已實例化、虛擬網路設定已異動、儲存設備存已被修改等。CimTrak for Docker/Kubernetes提供對容器部署設定的廣泛可視性。

領先的整合安全儀表板 SECURITY DASHBOARD

CimTrak的互動式圖形儀表板允許CimTrak使用者一目了然地查看其環境的狀態。 此外每個使用者可以自行定義其儀表板，以提供獨特的圖表，允許他們快速輕鬆地查看整個IT環境的狀態，或只是他們負責的系統。



易於與安全資訊與事件管理系統（SIEM）整合

如果您的組織使用SIEM技術，則可以輕鬆整合CimTrak收集的資料。CimTrak提供來自伺服器和其他終端的資訊。 CimTrak的檔案完整性監控（FIM）和設定監控提供及時的資訊以緩解攻擊與檢測其他異常所需的分析、關聯和情況感知。通過檢測系統狀態的實際異動，CimTrak補足了網路流量分析解決方案可能會錯過的事件。

透過CimTrak的日誌與稽核追蹤能力增強可監控的安全控制覆蓋範圍，以擴展SIEM的法規遵循報告。CimTrak 提供前所未有的捕獲證據輔助細節，還為SIEM的強大的數據挖掘引擎Data Mining Engine 增加重要資訊。這些技術的結合可以幫助簡化法規遵循報告並提高您的安全狀態。

CimTrak可與所有領先的SIEM解決方案整合（包括HP ArcSight、IBM QRadar、McAfee Enterprise Security Manager 、RSA Security Analytics與Splunk）整合，且都不需要任何復雜的配置或設定。

CIMTRAK REPORTS 報告

能夠提供異動資訊報告是非常重要的，如: 證明IT稽核的法規遵循、驗證發生的計劃異動以及讓所有IT運營人員了解情況。在企業中不同職能領域的個人通常需要不同詳細程度的不同報告。借助整合的報告引擎，CimTrak提供各種.pdf，.html和.csv報告格式，用戶也可以自行定義報告內容以顯示其組織特有的資訊。從全面詳細的更改報告到高級概述報告（適用於管理演示），CimTrak可為您提供組織所需的各種級別報告。

CIMTRAK TICKETING MODULE 票務模組

區分已知的"好"異動和應該調查的未知異動之間的差異，是您和您的團隊能大幅度地提昇反應異動事件時間的關鍵部分。CimTrak的SmartFIM™技術為用戶提供唯一的檔案完整性監控系統，可提供完全整合的異動票務系統。這讓各種規模的組織以符合經濟效益的成本，擁有執行計劃和記錄異動的能力。

此外，CimTrak整合的異動票務系統Change Ticketing System允許與現有的票務解決方案整合，例如CA Service Desk、Service Now、Cherwell 與Jira。

CIMTRAK 異動協調工作流程

使用CimTrak 可以更有效地管理企業範圍內的異動。 CimTrak 異動調節工作流程 Change Reconciliation workflow提供了一種無縫、易於使用的方法，從最初識別異動、調查與異動分類、將任務分配給工程師、最終補救與確認。CimTrak 異動協調工作流程提供了一個強大的工具集，用於分析異動的性質、執行惡意軟體分析、驗證異動是否為作業系統修補程式OS patch的驗證元件、記錄已完成操作及由誰執行操作的簡單方法。

CIMCOR

CimTrak產品商標為 Cimcor公司所有
了解更多產品資訊，請洽:台灣地區代理商 商丞科技股份有限公司 (02) 2914-8001

與威脅 THREAT FEED 整合

CimTrak與STIX 1.0 / 2.0和TAXII Thread Feeds整合，這種持續不斷的威脅資料流為CimTrak提供額外的資料，可以更好地洞察您的組織。隨著從威脅源下載新威脅的 hashes，CimTrak會自動使用惡意軟體/威脅Hashes malware / threat hashes更新其黑名單。只要有異動時CimTrak就會確認這些異動或新檔案不在黑名單中。此外，隨著新威脅的識別，CimTrak將主動檢查所有受監控系統，以確保新識別的威脅尚未在目前系統上。

即時檔案與惡意軟體分析
REAL-TIME FILE & MALWARE ANALYSIS

當檔案發生異動時，CimTrak可以與Virus Total、Palo Alto Wild fire或Checkpoint的威脅API整合，對檔案異動進行即時分析。結合CimTrak信任檔案註冊表CimTrak Trusted File Registry，現在比以往更容易識別檔案是否是惡意的。 此資料可用於動態更新CimTrak黑名單Blacklist，並自動檢查CimTrak監控的其他系統上是否存在惡意資料。

通過統一管理視圖輕鬆擴展

可以透過CimTrak Clustering將多個CimTrak Master repositories 主儲存庫叢集在一起，以水平擴展CimTrak。這種技術使CimTrak能夠滿足最大型基礎設施的需求。 叢集後CimTrak會自動啟用整合圖表功能，為用戶提供強大的“單一窗格” “Single Pane of Glass”，用於管理設定、建立政策以及檢查與安全相關的事件。

TRUSTED FILE REGISTRY™ 信任檔案註冊表

CimTrak的SmartFIM™技術是正在申請專利的CimTrak Trusted File Registry™的一個關鍵元件。這種高度創新的解決方案幾乎消除其它供應商的修補程式與更新 patches and updates（例如 Windows 和 Red Hat Linux的更新）所引起的誤報 False Positives。

通過自動提升Promoting修補程式與更新 patches and updates的權威基線 Authoritative Baseline，真正重要的異動浮出水面，大大減少了調查異動與最大化用戶IT環境安全性所花費的時間。

CIMCOR

了解更多產品資訊，請洽:台灣地區代理商 商丞科技股份有限公司 (02) 2914-8001

支援的平台

CIMTRAK FOR 伺服器、關鍵工作站與POS系統

» Windows: XP, Vista, 7, 8, 10, Embedded for Point of Service (WEPOS), POSReady
» Windows Server: 2003, 2008, 2012, 2016, 2019
» Sun Solaris: x86, SPARC
» Mac: Intel, Power PC
» Linux: Amazon, CentOS, ClearOS, Debian, Fedora, Oracle, Red Hat, SUSE, Ubuntu, others
» HP-UX: Itanium, PA-RISC
» AIX

WINDOWS 監測參數

» File additions, deletions, modifications, and reads
» Attributes: compressed, hidden, offine, read only, archive, reparse point
» Creation time
» File opened/read
» Group security information
» Local security policy
» Services
» DACL information
» File Size
» Installed software
» Modify time
» User groups
» Drivers
» File type
» Local groups
» Registry (keys and values)

UNIX 監測參數

» File additions, deletions, and modifications
» Attributes: read only, archive
» File Size
» Modify time
» Access Control List
» Creation time
» File type
» User and Group ID

支援的平台

CIMTRAK FOR NETWORK DEVICES 網路設備

» Cisco » Check Point » Extreme » F5 » Fortinet » HP » Juniper » Netgear » NetScreen » Palo Alto » Others

支援的平台

CIMTRAK FOR DATABASES 資料庫

» Oracle » IBM DB2 » Microsoft SQL Server » MySQL

監測參數

» Default Rules
» Groups
» Stored Procedures
» User defined data types
» Full text indexes
» Index definitions
» Table definitions
» Users
» Views
» Functions
» Roles
» Triggers

支援的虛擬化管理程序

HYPERVISORS CIMTRAK VMWARE ESXI 設定監控器

» VMware ESXi 3x, 4x, 5x, 6x

CIMCOR

了解更多產品資訊，請洽:台灣地區代理商 商丞科技股份有限公司 (02) 2914-8001

Cimtrak檔案完整性監控（FIM）與其他公司產品比較表

功能	CimTrak	其他公司FIM產品	說明
Real Time Integrity Monitoring 及時檔案完整性監測	支援	支援	
具備即時修復異動與完全防止更改能力	支援	不支援	
支援 Windows、Linux、UNIX	支援	支援	
支援 IBM DB2, Microsoft SQL Server,MySQL, Oracle等資料庫	支援	部份支援	
監測 Windows Registry	支援	部份支援	
監測 Point of Sale (POS) Systems	支援	部份支援	
監測網路設備	支援	部份支援	
監測 PCI 設定	支援	部份支援	協助符合PCI-DSS規範要求
監測 VMware ESX / ESXi 設定	支援	部份支援	
監測 Active Directory/LDAP	支援	部份支援	
監測 Google Compute Engine、Azure與 Amazon AWS等雲端設定	支援	部份支援	
監測 Docker / Containers 設定	支援	不支援	
Trusted File Registry 信任軟體與系統更新	支援	支援	自動識別供應商驗證的修補程式與更新，防止誤判發生
監測檔案內容與所有屬性	支援	部份支援	
通用標準認證 CC EAL Level 4+	支援	不支援	美國國防資訊系統局統一能力批准的產品清單
可即時恢復 SNMPv3 設備設定	支援	不支援	
異動發生時產生增量快照 Incremental Snapshots	支援	不支援	
偵測異動並自動反轉復原	支援	不支援	
可設定為拒絕權限 Deny Rights，阻止異動行為	支援	不支援	透過管理員權限，也無法更改
可比較異動(更改、新增、刪除)資料	支援	部份支援	

Cimtrak是業界唯一同時提供即時異動偵測、自動復原與防止覆蓋竄改功能的檔案完整性軟體。

進一步產品資訊，請洽:台灣地區代理商 商丞科技股份有限公司 (02)2914-8001